TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

2,00 €
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

HACKER JOURNAL

n.157
www.hackerjournal.it

ATTACCO CONTO TERZI

Come *TI INFETTANO* tramite un sito

MULTICS

Il *NONNO* del Pinguino



SENZA TRACCIA

Tutto ciò che devi sapere per *NAVIGARE SENZA VOLTO*

Wii SOTTO ATTACCO

Tutti i modi in cui hanno *CRACKATO* la *CONSOLE* più *VENDUTA AL MONDO*

QUATTORD. ANNO 8 - N°157 - 7/27 AGOSTO 2008 - € 2,00
WLF PUBLISHING

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

La forza di **Apple**

La forza di Apple
"Si può resistere alla forza di un esercito; non si può resistere alla forza di un'idea."
Victor Hugo (1802-1885)

Che Apple se ne faccia un baffo delle leggi di mercato e alle volte anche della decenza non c'è dubbio alcuno ma che addirittura i due più importanti gestori di telefonia mobile italiani si facciano mettere i piedi in testa da l'idea della forza di Cupertino in questo momento.

Stiamo parlando degli spot televisivi per il lancio dell'iPhone, per chiunque conosca un po' la comunicazione di Apple è risultato subito chiaro che la campagna arriva direttamente dall'ufficio marketing di Steve Jobs ma la cosa sconvolgente è che Tim e Vodafone abbiano accettato di avere lo stesso, medesimo spot con la sola differenza del loro logo al termine e rigorosamente prima di quello della mela. Non sappiamo e non vogliamo sapere quale altri accordi i due gestori abbiano dovuto accettare per avere la distribuzione iniziale dello smartphone con la mela sopra ma deve essere stato divertente vedere il direttore generale di Tim che chiede a Steve Jobs di marchiare l'iPhone con il logo Tim, soprattutto ci sarebbe piaciuto avere la trascrizione della risposta...

BigG

CONTINUA LA CACCIA

In tanti ci hanno già risposto ma non ci basta mai e vogliamo solo il meglio per le nostre pagine e i nostri lettori e quindi continuate a mandare le vostre candidature alla mail:

contributors@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.157
7 / 27 agosto 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

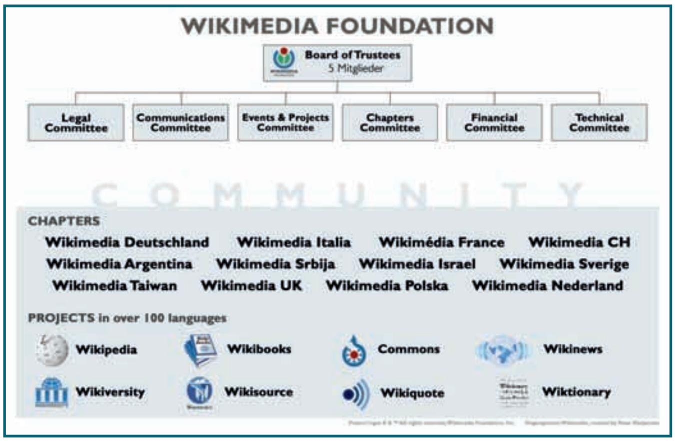
Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

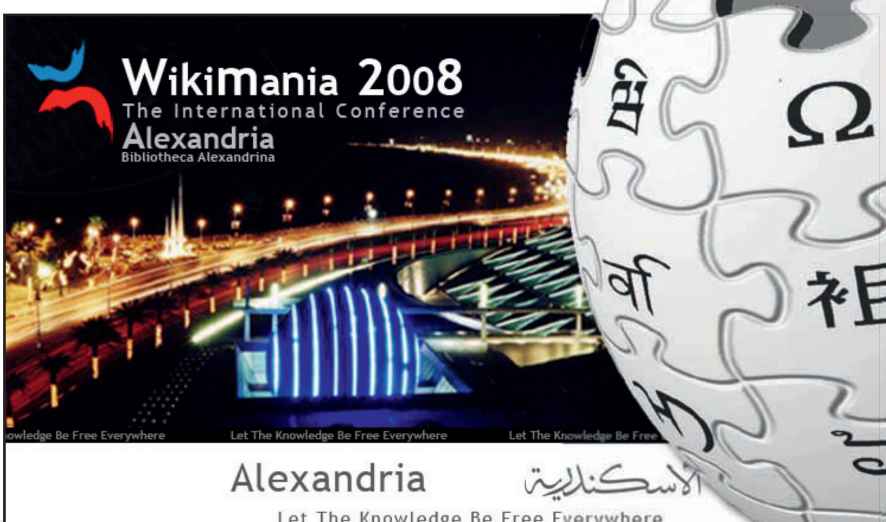
RIVOLUZIONE Wiki



Il mese scorso si è tenuto l'annuale raduno dei contributors della famosa enciclopedia libera con oltre 600 partecipanti. Il luogo stabilito per il raduno è stato quanto meno evocativo, Alessandria d'Egitto nella quale circa 2.000 anni fa si trovava la più grande biblioteca del mondo.



Il tema più acceso di discussione durante la manifestazione è stato il concetto base della stessa enciclopedia, la libertà di chiunque di inserire nuove voci o correggere quelle già esistenti. Che questo sistema sia la forza ma anche il più grande difetto, in quanto fonte di infiniti problemi, di Wikipedia è chiaro già da tempo ma da qua a trovare una soluzione ce ne passa, anche perché la stessa enciclopedia ha sempre rifiutato di agire da controllore, cosa che le ha anche permesso di rigettare ogni tipo di accusa derivante dai contenuti, a volte diffamatori e lesivi della privacy pubblicati in essa. La proposta uscita dal raduno Wikimania 2008 è stata quella di avvalersi di un nuovo sistema di controllo, in definitiva verranno incaricati alcuni utenti che si troveranno a vagliare i contenuti riguardanti argomenti di cui sono comprovati esperti e questi contenuti non diventeranno pubblici fino alla loro approvazione da parte di questi editor. In definitiva si profila una sorta di gerarchia tra i contributors di Wiki che potrebbe in ogni caso portare alcuni utenti ad allontanarsi dall'amata enciclopedia "anarchica". Per ora il nuovo sistema è operativo solo sulle pagine di wiki in Germania e presto saranno disponibili i risultati di questo esperimento, staremo a vedere. ■







WINDOWS XP NON MOLLA

Con il 30 giugno e la cessazione delle vendite di Windows Xp sembrava ormai calato il sipario sul più apprezzato dei sistemi operativi di Microsoft.
Ma Windows Xp sembra però piuttosto resistente e non vuole decidersi a riposare in pace, grazie anche alla complicità di quello che è probabilmente il più famoso negozio online: Amazon.
Nella classifica dei software più venduti su Amazon spiccano Windows Xp Professional e Home, aggiornati al Service Pack 2 e venduti a 204,27 e 183,99 dollari.

IPHONE UNA MALATTIA

In coda due giorni prima per acquistare l'iPhone. Alla fine il melafonino è sbarcato anche in Italia e in Asia, dove l'attesa sembrava più fremente che da noi in fatti fuori dai negozzi ufficiali si sono viste molte persone armate di un cartello che diceva: "We Love iPhone".



"Ciò che di più attira in un iPhone è che si tratta di un prodotto Apple": parole di Hiroyuki Sano, ventiquattrenne giapponese che dalla mattina di mercoledì 9 luglio ha aspettato fuori da un negozio di Tokio, ben due giorni prima della messa in vendita.

Che ci sia gente disposta a passare due giorni all'aperto pur di avere un telefonino non appena questo sarà disponibile dev'essere normale in quella lontana nazione, visto che per recarsi all'appuntamento Sano ha ottenuto il via libera da un suo professore, anch'egli fan della mela, che gli ha concesso di non studiare per potersi concentrare sulla missione.

ERRATA CORRIGE

Anche i migliori sbagliano... figuratevi noi della redazione...
E così sulla copertina del numero scorso ci siamo vantati di avere un'intervista con Demonoid che purtroppo invece non compare nelle pagine interne. Scusandoci di quanto è accaduto vi consigliamo di leggere l'intervista a pagina 8 di questo numero... Questa volta c'è!!!



EMULE & CO. N° 2

Per tutti gli amanti del P2P non possiamo non consigliare di andare a prendere in edicola Emule & Co.
Trovate proprio in questi giorni in vendita il numero due ricco di trucchi, consigli e novità sul mulo e su tutto ciò che riguarda il filesharing.



HOMER VIRUS

Il problema è sorto quando qualcuno ha creato su AIM l'account chunkylover53, i fan hanno subito incominciato a scrivere a questo indirizzo, al quale rispondeva Matt Selma, sceneggiatore e produttore della saga dei Simpson.
L'account rimase però inattivo per un po' di tempo, facendo rimanere con il fiato sospeso i fan, che speravano di chattare con Homer.
Dopo qualche tempo l'account si è



HOT NEWS

CHRYSLER WI-FI

Dall'anno prossimo il costruttore americano di automobili Chrysler immetterà sul mercato 20 modelli di veicoli marchiati Chrysler, Dodge e Jeep dotati di connettività Bluetooth e Wi-Fi.
Sfruttando anche un disco da 30 Gbyte, i passeggeri potranno così sincronizzare le rubriche dei loro cellulari mentre l'autista potrà controllare l'iPod per mezzo dei comandi al volante. Inoltre su uno schermo touch screen appariranno le informazioni sul traffico, mentre per governare i vari dispositivi senza usare le mani è prevista anche l'implementazione del controllo vocale.
Unica nota negativa di tutto questo progetto sarebbe la lentezza delle connessioni via rete cellulare: un bel supporto WiMax sarebbe forse più indicato per chi già spende un bel patrimonio per l'auto.

LA TUA GMAIL SI VEDE CON ALTRI?

Una nuova funzione permette di visualizzare chi sta accedendo alla nostra casella di posta e chiudere le sessioni dimenticate aperte di cui curiosi e malintenzionati potrebbero approfittare.

Google ha implementato un nuovo servizio per controllare gli accessi alla propria casella di posta. Il servizio, inizialmente disponibile solo nella versione americana e ora utilizzabile anche in quella italiana, permette di creare un log tutte le volte che la vostra casella e-mail è stata aperta.
Ora tramite una linea di testo posta al fondo della pagina, sotto la capienza della casella, è possibile visualizzare se qualcun altro sta visionando il nostro account e quando è avvenuto l'ultimo accesso.



PERICOLO SU DNS

La scoperta risale a sei mesi fa ma prima di rendere pubblica la notizia si è preferito realizzare le correzioni per tutte le maggiori piattaforme.
Esiste una falla nel protocollo Dns che è potenzialmente pericolosa: un suo sfruttamento potrebbe far aumentare enormemente gli attacchi di phishing, dirottando gli utenti verso false pagine web.
Il protocollo Dns è fondamentale per il funzionamento di Internet: i server Dns hanno infatti il compito di tradurre gli indirizzi mnemonici in indirizzi numerici e viceversa, permettendo così la facile navigazione tra le pagine web cui siamo abituati.
I dettagli, in ogni caso, saranno resi pubblici solo tra circa 30 giorni, mentre le patch, anche se sottoposte a reverse engineering, non dovrebbero permettere di capire quale sia la vulnerabilità; almeno così sostiene Dan Kaminsky, lo scopritore.

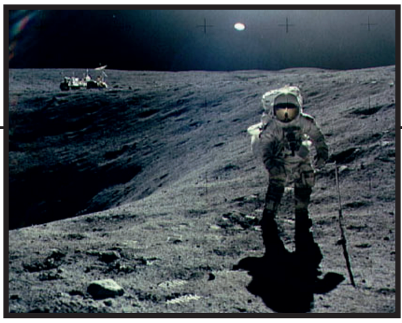
riattivato, inviando a tutti i contatti il trojan kimya.exe e dicendo che il programma serviva a vedere un episodio del cartone animato.



Il software però manda messaggi di errore particolari e infetta il Pc, aprendo delle porte Tcp per le connessioni remote e permettendo a un malintenzionato di sfruttate il computer infetto a suo piacimento.

WEB ANCE PER I CIECHI

Si chiama WebAnywhere: è stato sviluppato da uno specializzando dell'Università di Washington ed è un applicativo Internet che rientra nel sempre più ampio novero degli strumenti che agevolano la navigazione sul Web per chi non vede. Si tratta di un browser specializzato, una soluzione con cui lo sviluppatore, Jeffrey Bigham, spera di consentire ai non vedenti di controllare velocemente l'orario di un volo su qualsiasi computer, di navigare in aeroporto, di pianificare un giro turistico specializzato o di scrivere rapidamente una email in un qualsiasi internet cafè. L'unica difficoltà è il primo avvio: se il computer non è già predisposto per offrire il feedback verbale tramite l'applicativo, lanciarlo potrebbe non essere facile per chi è privo della vista. Ma su questo aspetto Bigham è fiducioso: i non vedenti sono spesso sagaci e profondi conoscitori delle scorciatoie di tastiera e sanno chiedere aiuto.



URINA RIUTILIZZABILE

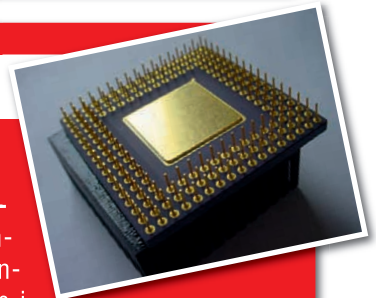
La gestione dei rifiuti liquidi e solidi prodotti dagli astronauti rappresenta una delle voci di costo più impegnative. Comprensibile dunque il fatto che NASA tenti di continuo di sperimentare e migliorare le tecnologie a disposizione.
Ora il programma Orion mira a raccogliere l'equivalente di circa 30 litri di urina al giorno per una decina di giorni. Si tratta di liquidi che devono essere introdotti nel sistema di analisi approntato all'SLC di Houston, dove la NASA chiede a impiegati e visitatori di donare la propria urina nel periodo compreso tra il 21 e il 31 luglio.
La raccolta di urina, sulla quale verranno testate nuove tecnologiche di elaborazione, servirà a progettare nuovi metodi e procedure di gestione dei rifiuti liquidi umani.

400 GB PER TOSHIBA

Il prossimo settembre Toshiba lancerà un nuovo hard disk da 2,5 pollici, l'MK4058GSX, che porterà la capacità dei suoi dischi per notebook a 400 GB, 80 GB in più dell'attuale modello top di gamma. Anziché allinearsi alla concorrenza, e sfoderare da subito un'unità da mezzo terabyte, il colosso giapponese ha dunque preferito procedere per gradi: questa scelta, a suo dire, trova giustificazione nella volontà di focalizzarsi su aspetti quali affidabilità, risparmio energetico e silenziosità.
L'azienda afferma inoltre che il proprio disco riduce la rumorosità di 2 decibel e i consumi del 20%. Queste caratteristiche sono sempre più importanti non soltanto per i notebook, ma anche per i PC small form factor, le set-top box e i server blade.



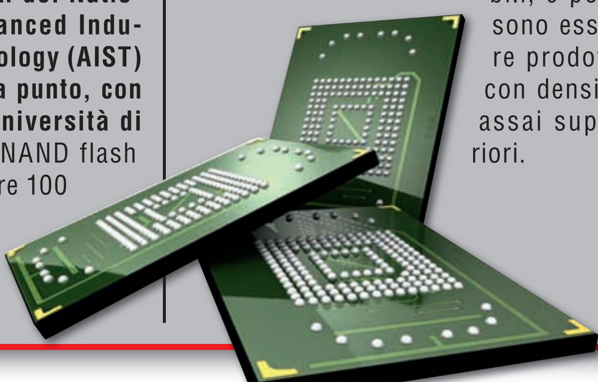
ENTRO DALLA CPU



Si puo' attaccare un Pc sfruttando una vulnerabilita' della Cpu, indipendentemente dal sistema operativo utilizzato. Kris Kaspersky ha annunciato che all'Hack In The Box Security Conferenze 2008 di ottobre dimostrerà di poter attaccare i microprocessori dei Pc tramite javascript e pacchetti Tcp/Ip. Questi tipi di attacchi sarebbero indipendenti dal sistema operativo e verranno sferrati su Windows Xp, Vista, Windows Server, Linux, BSD e Mac OS X. I processori Intel sui quali verrà fatta la dimostrazione presentano adesso 35 bug conosciuti che sono stati resi pubblici, anche se l'azienda produttrice ha già fornito le soluzioni per risolverli. Bisognerà vedere quali altri processori siano vulnerabili.

CHIP FLASH PER 100 ANNI

Un gruppo di scienziati del National Institute of Advanced Industrial Science and Technology (AIST) sostiene di aver messo a punto, con la collaborazione dell'Università di Tokyo, chip di memoria NAND flash in grado di sopportare oltre 100 milioni di riscritture, con una vita media stimata di 100 anni. Dulcis in fundo, questi chip assorbono oltre tre volte meno energia di quelli tradizionali, contribuendo così a migliorare l'autonomia dei dispositivi mobili, e possono essere prodotti con densità assai superiori.



TECH-PRO.NET
BANDITO PER ERRORE

Messo alla gogna in rete per un errore di valutazione di McAfee. Tech-Pro.net, un sito che ospita recensioni e vende software, sta facendo i conti con un isolamento che dura da due settimane, un esilio originato da un errore di valutazione e dalla collaborazione tra Yahoo e il servizio di sicurezza. Il servizio SiteAdvisor di McAfee, sul-



YOU TORRENT RELOAD

You Torrent riparte dal file sharing autorizzato. Il motore di ricerca che a gennaio stupì per la sua crescita repentina si era dovuto fermare a causa del richiamo all'ordine dei proprietari del copyright sui contenuti, promettendo poi al suo pubblico di voler tornare più in forma che mai dopo opportuna purga.

YouTorrent è ora un meta-motore di motori di ricerca di torrent "buoni" come Vuze, lo stesso BitTorrent, LegalTorrents, Legittorrents e via di questo passo. Oltre alla quantità, il search engine fa professione di contenere qualità: "Ora forniamo dati accurati sui seed e i peer e i risultati sono facili e veloci da navigare, e più in linea con le tradizionali pagine dei risultati dei motori di ricerca" sostiene uno dei fondatori di YouTorrent.

CYBERGANG RUSSA

Coreflood Gang è il nome dato dagli esperti di sicurezza ad un flagello del cyber-crimine organizzato, una banda di cracker di matrice russa che da anni imperversa in rete con virulenza inaudita. La gang è specializzata nel furto di account bancari online, e i danni fin qui provocati appaiono ingenti.

La gang agisce in un modo ben noto a chi si occupa di sicurezza online, iniettando codice malevolo nelle pagine web, così da re-indirizzare l'utente inconsapevole verso server su cui è depositato il trojan bancario custom che ha il compito di raccogliere le preziose informazioni di e-banking quali username, password, numeri di carte di credito e codici di autenticazione a doppio fattore.

NINTENDO WII VINCE

Nessun rallentamento, nessuna flessione: le vendite della Wii, la console videoludica di Nintendo, continuano a tenersi alte, ai massimi livelli, anche negli Stati Uniti, un mercato che certo non ha girato la testa alla Xbox 360 di Microsoft né alla più recente Playstation 3 di Sony.

Eppure, dicono gli esperti di NPD Group, dopo "appena 20 mesi, Wii è il nuovo leader di vendite negli Stati Uniti con quasi 10,9 milioni di unità vendute".

Fino a giugno, la piattaforma più venduta era Xbox 360, spodestata nel corso del mese grazie alla consegna di 666.700 console da parte di Nintendo. Nel mese di giugno sono state vendute poco più di 405mila Playstation 3, e questo anche a fronte del rilascio di un titolo di grande richiamo, come il nuovo capitolo di Metal Gear Solid. Xbox 360, sul mercato da molto più tempo, è stata acquistata 219.800 volte.

FEDELI OCCHIO ALLA RETE!

Il Santo Padre mette in guardia i giovani: i mezzi di comunicazione e Internet danno spazio a violenza e intolleranza, sminuiscono il significato di valori e banalizzano la realtà. Benedetto XVI si è così rivolto alla folla di papaboys che affollavano il molo di Barangaroo, nei dintorni di Sidney, per partecipare alle manifestazioni in programma per la celebrazione della Giornata Mondiale della Gioventù. La virtualità, spiega il papa nel discorso rivolto ai giovani, è spesso veicolo dell'esaltazione della violenza e del degrado sessuale, che vengono presentati spesso dalla televisione e da internet come divertimento.

la base di test e di segnalazioni degli utenti, all'inizio di luglio aveva rilevato delle attività sospette su Tech-Pro.net: pareva fornire dei download che avrebbero potuto attentare alla sicurezza degli utenti. Ma l'allerta di McAfee non ha messo in guardia i soli netizen che usufruiscono del servizio della security company: Yahoo, che da poche settimane si affida ciecamente alle liste stilate da SiteAdvisor, ha provveduto a contrassegnare come pericolose alcune pagine del dominio nei propri risultati di ricerca.

CHIAVE USB O CAVO?

Spesso le flash drive USB sono vere e proprie banche di dati sensibili, un posto sicuro dove tenere tutto ciò che serve a portata di mano, sempre e comunque. Capita però che qualche buontempone decida di rubare il prezioso device. Come dissuadere le manoleste? Un'idea è Hacked!

La sua forza sta proprio nell'aspetto. Si presenta come un normale cavo USB tranciato a metà, con tanto di fili in bella vista. L'idea è che i 2 gigabyte che nasconde non facciano gola a nessuno.



Il suo designer Windell Oskay ritiene che la tattica del qui sono già passati sarà un successone. Per il momento non sono ancora disponibili info relative alla commercializzazione e al prezzo del device sul sito del produttore Fred&Friends.

DEMONOID: PERSEGUITATO... SI rifugia nell'Est!

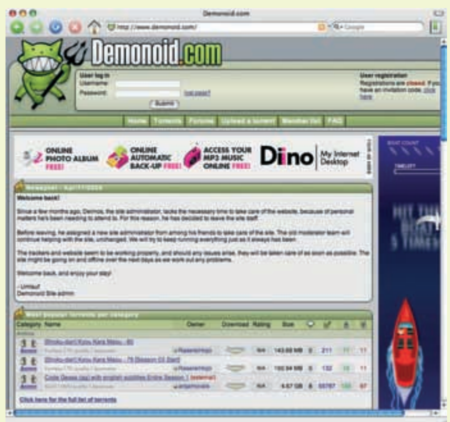


Creato da un personaggio noto solo con lo pseudonimo di Deimos, Demonoid è un tracker BitTorrent privato, il più importante per quanto riguarda le fonti francofone. Il sito dà accesso a migliaia di file (film, album,

Demonoid è il secondo maggiore tracker BitTorrent della Rete, con i suoi 100.000 file indicizzati e i suoi 3 milioni e mezzo di utenti regolari, e si colloca al 403° posto tra i siti più visitati di Internet. Naturalmente, nel turbine delle azioni legali delle major e delle associazioni delle case discografiche e cinematografiche, Demonoid non poteva sfuggire all'ondata repressiva che si è scatenata sui siti di questo tipo. The Pirate Bay è in attesa di processo in Svezia, TorrentSpy è scomparso e Mininova si prepara a una grande battaglia giudiziaria...

:: Demonoid in Olanda...

Solo un anno fa, questo tracker privato era ospitato da un server nei Paesi Bassi. Il sito è classificato come "privato" in quanto prevede un'iscrizione obbligatoria che può essere ottenuta solo dietro presentazione o qualora le risorse lo consentano. Ma il 26 giugno 2007 la BREIN (equivalente olandese della SIAE) ordina al server di Demonoid di bloccare il sito (con 50.000 euro di ammenda per ogni giorno di ritardo). LeaseWeb, dopo aver tentato di glissare, chiude il sito e comunica il nome e l'indirizzo del suo amministratore storico, Deimos. Previdente, Deimos ha pensato bene di trasferire la base di dati del sito in un altro Paese. È per questo che meno di una settimana dopo aver chiuso i battenti, Demonoid riapre a Laval, in Canada, nella provincia di Quebec. L'obiettivo è chiaramente quello di sfuggire alla legge olandese sulla proprietà intellettuale. La BREIN, che definisce questo comportamento "giocare a nascondino", non abbandona la lotta e ci sono buone ragioni per ritenere che i problemi incontrati in seguito nel Canada siano stati creati proprio da questa organizzazione.



Sito xxxxxxxxxxxxxxxx

:: ...e poi nell'ex-Unione Sovietica...

In effetti, qualche mese dopo, la CRIA (l'equivalente della SIAE in Canada) inizia a lamentarsi e chiede a Demonoid di cessare le sue attività. Per tutta risposta, il sito blocca ogni accesso dal Canada (così come isoHunt e TorrentSpy avevano bloccato l'accesso ai loro siti da parte dei navigatori ame-

ricani per evitare guai con la RIAA). Lo scorso 9 novembre il sito Web è stato chiuso, con una pagina che spiega che "La CRIA ha minacciato l'azienda che ci ospita e per questa ragione non ci è possibile rimanere on-line. Spiacenti per il disguido, vi ringraziamo per la vostra comprensione". Deimos aggiunge che vari problemi (personali e finanziari) "gli impediscono di trovare una soluzione nell'immediato". Sembrava proprio la fine. L'ultimo colpo di scena risale al 10 aprile scorso. Deimos annuncia che "abbandona il posto di amministratore di Demonoid, passando il timone a un amico intimo di cui si fida completamente". Una settimana dopo, gli utenti ricevono una e-mail che li informa che Demonoid ha riaperto in un Paese dell'ex-blocco comunista: l'Ucraina (vedi nostra intervista esclusiva di seguito).



Petro Vlasenko, direttore commerciale

PRIVET UCRAINA INTERVISTA AL NUOVO GESTORE DI DEMONOID

Dopo tre ore di aereo siamo arrivati a Kiev, capitale dell'Ucraina nonché sede del nuovo server di Demonoid, ColoCall. Nella sede, situata in pieno centro, il direttore commerciale Petro Vlasenko ha

Siete al corrente della storia di Demonoid e delle sue disavventure giudiziarie in Olanda e in Canada?

PV In generale sì ma ovviamente non conosciamo tutti i particolari.

In che modo il gruppo di Demonoid si è messo in contatto con voi?

PV Hanno semplicemente cliccato su una delle nostre numerose pubblicità Google Adwords che descrivono i vantaggi delle nostre soluzioni di hosting "offshore". Sono clienti come gli altri. Comunichiamo via e-mail, in inglese.

Come è avvenuto il trasferimento di questa grossa base di dati?

PV Non ne sappiamo nulla, gli amministratori di Demonoid hanno semplicemente affittato lo spazio di archiviazione e hanno fatto tutto da soli.

Qual è il quadro giuridico in Ucraina? Temete qualche ripercussione?

PV Noi ospitiamo soltanto file torrent. In Ucraina non c'è nulla di illegale in questo. Non esistono nemmeno precedenti giuridici per questo tipo di casi. In ogni caso, siamo rispettosi della legge e se la giustizia ci chiederà di non lavorare più con Demonoid, interromperemo la collaborazione. I responsabili di Demonoid ci hanno chiesto di informarli se sentiremo cambiare il vento...

> "I responsabili di Demonoid ci hanno chiesto di informarli se sentiremo cambiare il vento..."

Cosa pensate dell'ingresso dell'Ucraina nell'Organizzazione Mondiale del Commercio?

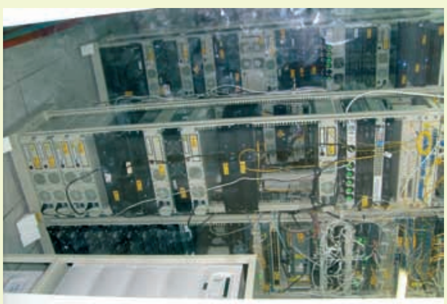
PV Penso che ci siano problemi molto importanti da risolvere in Ucraina a fronte dell'ingresso nel WTO. Vedremo...

Avete altri clienti nell'ambiente del peer-to-peer o in altre "zone grigie"?

PV Sì, qualche sito russo o ucraino ma nessuno delle dimensioni di Demonoid. Ospitiamo anche siti di dissidenti e oppositori politici russi e bielorussi. Ultimamente abbiamo ospitato anche un sito di Hamas. La CIA si è risentita e ha chiesto all'SBU (il servizio segreto ucraino) di effettuare un'inchiesta. Sono venuti nella nostra sede e hanno concluso che era tutto in ordine...

Perché il sito non è accessibile dagli IP ucraini? È una condizione imposta da voi?

PV [L'interlocutore appare sorpreso] Non ne so nulla e non è dovuto alla nostra volontà. [NDR: infatti, questo filtraggio selettivo è sicuramente opera dello stesso Demonoid, che senza dubbio mira a evitare qualsiasi tensione con il governo del Paese che lo ospita].



di ColoCall, il nuovo server ucraino di Demonoid

Demonoid.com

A volte ritornano: MOCA2008



A fine agosto si svolgerà a Pescara la seconda edizione del Metro Olografix Camp, per gli amici MOCA2008

In molti ci speravano, in pochi ci credevano, le voci erano discordanti, gli animi accesi, ma alla fine ci sono riusciti! Dopo quattro anni dalla celebrazione dei 10 anni di vita dell'associazione, la Metro Olografix (**http://www.olografix.org**), a grande richiesta terrà un nuovo camp estivo, un nuovo **MOCA** (Metro Olografix CAmp). L'appuntamento è dal 21 al 24 Agosto 2008, presso il Parco "ex Caserma Di Cocco" e come quattro anni fa sarà "un hacker camp in stile nord-europeo, ad accesso libero e gratuito", all'insegna del divertimento e della condivisione delle informazioni e del sapere.

Questa la meravigliosa cornice che ospitera l'appuntamento di quest'anno del Moca.



La pagine ufficiale del MOCA 2008 dove potrete recuperare tutti i dati sulla manifestazione che si terrà a Pescara.

Il MOCA2008 sarà un'occasione per "incontrare vecchi e nuovi amici, tutti coloro che hanno popolato l'underground telematico in questi anni e che sono pronti a viverlo nel prossimi anni, assieme a chi si sta affacciando ora su una realtà telematica sempre più preoccupante per via delle implicazioni tecnologiche e legal"i.
Il tutto in un'area di campeggio in cui sono tutti be nvenuti con la propria tenda ed il proprio computer per (come si legge sul sito) "smanettare, sperimentare, giocare, chiacchierare, fare qualsiasi cosa ci permetta di tornare a casa pensando "anche questa volta, ne valeva davvero la pena!"

Nicola D'Agostino

QUATTRO ANNI FA

Per chi voglia ripercorrere o capire cosa sia stato il MOCA sul sito della Metro Olografix c'è un'intera area della gallery (http://www.olografix.org/index.php?spgmGal=Metro_Olografix/Eventi/MOCA_2004&page_id=82) con decine e decine di foto che mostrano le iniziative, il campeggio, le follie (una su tutte: il lancio dell'hard disk) ma anche la preparazione e la smobilitazione del primo MOCA, tutte gestite da volontari arrivati da tutta Italia prima dell'apertura e trattenutisi dopo la conclusione.

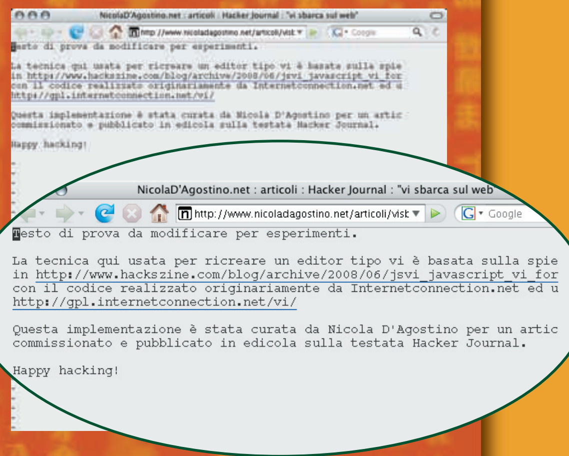


la bandiera "piratesca" della metro olografix che sventolava sul primo MOCA

Per maggior informazioni vedere il sito web http://camp.olografix.org/home.php su cui è già attiva l'iscrizione (http://camp.olografix.org/home.php?goto=3&lng=) che serve esclusivamente per dimensionare i servizi del camp (tra cui i bagni).

Vi sbarca sul Web

Qualche riga di HTML e si può trasformare un banale form sul proprio sito web o blog in qualcosa di originale e "old sk00l"



Per chi volesse vedere e provare, una dimostrazione è online all'indirizzo www.nicoladagostino.net/articoli/visbarcasulweb.html

Per chi vuole scrivere e modificare testi come un vero smanettone Unix le scelte sono poche: Emacs o Vi. Ora chi non ne può fare a meno o vuole fare uno scherzo da geek ai suoi visitatori può infilare Vi anche nei form di una pagina web trasformando una finestra o un tab del browser in una sessione di videoscrittura a linea di comando.

:: Benvenuti in jsvi

L'idea è venuta al provider Internetconnection.net che ha attrezzato una pagina dimostrativa (http://gpl.internetconnection.net/vi/) tramite cui scrivere, modificare, salvare (i comandi sono quelli di vi, ovviamente) e stampare del testo.

:: Inserire immagine jsvi.tiff

Qui si apprende che l'implementazione si chiama jsvi, che è rilasciata con licenza GPL3 supporta quasi tutte le combinazioni di comandi di vi ed è in gran parte compatibile con il più moderno vim (Vi improved). C'è il controllo ortografico durante la digitazione, si integra con la clipboard del sistema operativo su cui è eseguito, e il codice è compatibile con numerosi browser, tra cui Firefox, Safari e Opera.

:: A casa nostra

Ancora più interessante è la possibilità di usare jsvi sul proprio sito web ad esempio nel modulo per commentare. L'idea è di Hackszine (http://www.hackszine.com/blog/archive/2008/06/jsvi_javascript_vi_for_web_for.html) che spiega gli ingredienti necessari: scaricare il file vi.js (http://gpl.internetconnection.net/vi/vi.js), includerlo nel documento HTML e poi richiamarlo in un form con textarea che si vuole far "gestire" da vijs. Aggiungiamo che è importante anche usare il css di Internetconnectione (http://gpl.internetconnection.net/vi/vi.css) pena problemi di visualizzazione.

Nicola D'Agostino

LA RIVINCITA DEL JAVASCRIPT

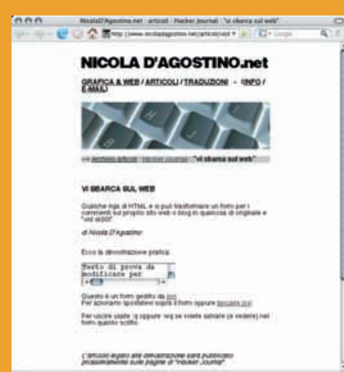
Javascript a lungo non ha goduto di buona fama: negli ultimi anni è però salito agli onori diventando una tecnologia di primo piano su cui poggia Ajax e tutto il cosiddetto "Web 2.0". Framework e librerie come scriptaculous o prototype hanno rivoluzionato le concezioni di cosa si poteva fare l'ECMAscript (questo il suo nome ufficiale) e questo linguaggio di scripting ha recuperato terreno non solo sul linguaggio a cui si richiamava nel nome, Java ma anche su Flash, con diversi effetti di grafica e manipolazione dell'interfaccia utente.

Nella pratica la pagina web deve avere nell'head queste due righe

```
<script src="http://indirizzoal/vi.js"></script>
<link rel=stylesheet href="http://indirizzoal/vi.css"
type="text/css">

e dentro il body:

<form>
<textarea name="body"
onfocus="editor(this);">
Testo di prova da modificare per
esperimenti.
</textarea> &lt;- Zona gestita da
jsvi. Spostatevi sopra oppure <a
href="" onclick="editor(document.
forms[0].elements.body);return
false;">lanciate jsvi</a>
</form>
```



ANONIMI E PROTETTI SUL WEB

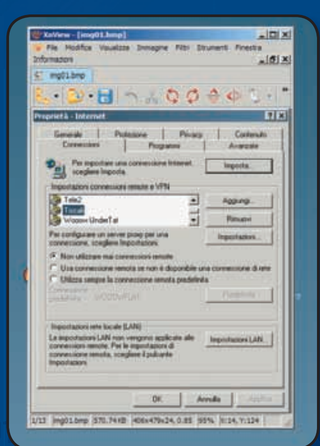


Navigare in sicurezza e al riparo da occhi indiscreti? Si può, e con pochi clic! Scopriamo tutte le opportunità offerte dai proxy e dai servizi di anonimizzazione

Privacy: se ne parla con insistenza, sopratuttto con riferimento a Internet. Gli allarmi hanno giustificazioni fondate: accedere al Web significa mettere a rischio dati personali di ogni genere, comprese quelle informazioni che possono essere raccolte analizzando le abitudini di navigazione. Possono sembrare dati inutili, ma in realtà offrono a spammer e malintenzionati vari l'opportunità di sferrare attacchi molto più mirati. La migliore strategia difensiva consiste nel nascondere le informazioni relative ai nostri dati e alle pagine che visitiamo e, su tutto, l'indirizzo IP, ovvero l'indicativo numerico assegnatoci al momento della connessione e che consente di risalire alla nostra identità. Per nasconderlo possiamo usare un proxy, ovvero un normale computer che "filtra" il traffico dei dati in entrata e in uscita.

:: Un po' di storia

I server proxy non sono nati con lo scopo di garantire l'anonimato. I primi, infatti, erano Transparent proxy, ovvero server che mantengono leggibile in chiaro il nostro IP. Il loro scopo era quello di bloccare i contenuti a rischio e ottimizzare il flusso dei dati attraverso una procedura chiamata caching. Il suo funzionamento si basa sulla memorizzazione dei dati che transitano sul server. Se ad esempio una pagina è già stata caricata in precedenza da un altro utente, il proxy la invierà direttamente senza effettuare una nuova richiesta al server che ospita i dati originali. Si tratta di una funzione usata soprattutto in passato, quando le connessioni a Internet raggiungevano al massimo i 56K. Con un collegamento del genere, il passaggio attraverso un proxy consentiva di ottenere un notevole risparmio di tempo. Anche questo tipo di server consentono di limitare la circolazione di informazioni riguardanti il nostro sistema, almeno per quanto riguarda il sistema operativo, il browser e la lingua che usiamo.



***Modem analogico o ADSL?** Se vogliamo impostare un proxy con Internet Explorer, dobbiamo distinguere le due situazioni: se usiamo un modem 56K facciamo riferimento alla singola connessione, se usiamo la banda larga dobbiamo invece cambiare le impostazioni della LAN.*

:: Anonimato

Un discorso diverso vale per gli Anonimity Proxy e gli High Anonimity Proxy, chiamati anche Elite. I primi nascondono il nostro IP, che verrà schermato e sostituito da quello del proxy. I secondi, invece, riescono addirittura a rendere irrintracciabile il transito attraverso un server intermedio, simulando una connessione diretta. In pratica, usando un normale proxy anonimo, chi dovesse provare a rintracciare la connessione si renderebbe conto che il vero IP è stato nascosto passando attraverso un server. Usando un proxy Elite, invece, il curioso di turno non avrebbe nemmeno questa possibilità e sarebbe portato a credere che si tratti di un normale collegamento da PC al Web.

DAVVERO ANONIMI?

Non illudiamoci: navigare in anonimato non implica un completo anonimato nel senso letterale della parola. I proxy a cui ci connettiamo conservano traccia degli accessi e dei relativi IP, permettendo di risalire comunque all'utente che ha richiesto la pagina Web. I dati non saranno a disposizione di chiunque, ma potranno essere forniti in casi di particolare gravità, per esempio su richiesta della magistratura in presenza di un'ipotesi di reato. Il braccio di ferro fra la lotta contro il crimine da una parte, sviluppo tecnologico e difesa della privacy dall'altra è del resto in pieno svolgimento, e ha persino contrapposto in sede processuale i ministeri più direttamente coinvolti sui due fronti. Quello attuale, comunque,

:: Solo per navigare

I limiti dei proxy riguardano il tipo di comunicazioni che possono "coprire", che si limitano alla navigazione via browser. Difficilmente funzioneranno coi programmi di Instant Messaging, mentre possiamo escludere in partenza di utilizzarli per schermare lo scambio di file tramite P2P. Per questi ultimi occorrono casomai software specifici come Ants o Mute. Per sapere con certezza se stiamo navigando in modalità anonima, connettiamoci a un sito concepito per visualizzare l'IP dei visitatori come www.mostraip.it. La pagina Web mostrerà il numero di IP e il provider che lo ha fornito. Se corrisponde al nostro fornitore di accesso, significa che la trasmissione dei dati sul Web avviene "in chiaro", mentre un riferimento a un server situato all'estero fornirà il responso opposto. Anche la presenza di indicazioni negative o generiche accanto alle voci sottostanti, ovvero al suppporto per ActiveX, cookies e JavaScript, costituirà un punto a favore del livello di anonimato e sicurezza della nostra connessione.

:: Impostiamo il browser

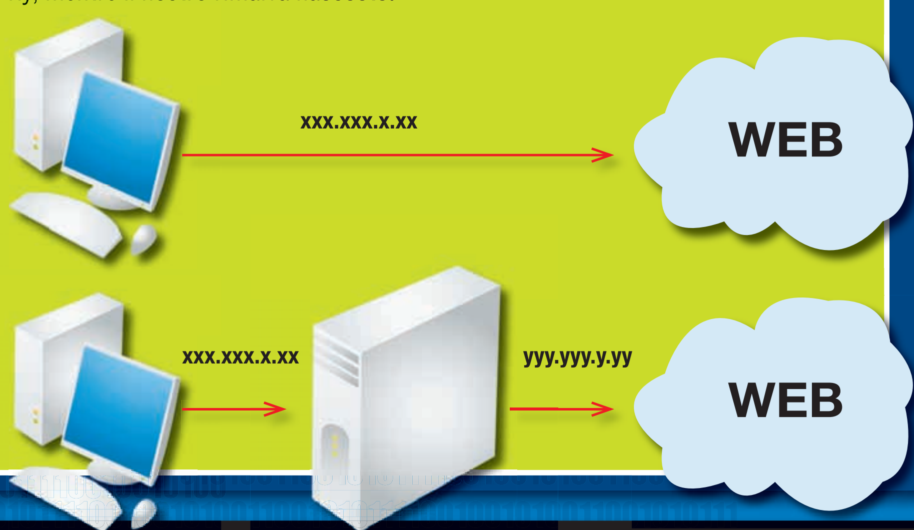
Navigare anonimi aumenta il livello di sicurezza, ma sarà inutile se lasciamo che cookies o script siano liberi di rivelare dati che dovrebbero rimanere nascosti. Per questo motivo è fondamentale che il browser da noi utilizzato venga configurato a tale scopo, riducendo al minimo le tracce che lasciamo quando navighiamo sul Web. L'esempio riportato nell'articolo si basa sulla recente versione 3.0 di Mozilla Firefox, ma può essere applicato con altrettanta efficacia a Opera, K-Meleon e ad altri software di terze parti. Internet Explorer non dispone invece di strumenti altrettanto efficaci per gestire i dati di navigazione, per cui rimane una soluzione poco consigliabile, così come lo sono i browser che sfruttano lo stesso "motore", come Avant o Maxthon. Diversa anche la gestione dei del proxy: Firefox e gli altri browser dispongono di opzioni autonomamente configurabili, mentre il browser di casa Microsoft condivide le impostazioni del sistema. Si tratta di un dettaglio tutt'altro che trascurabile: usando i primi, infatti, potremo navigare anonimamente e continuare a usare programmi di P2P o per i messaggi istantanei. Con Internet Explorer, invece, la scelta di usare un proxy impedirebbe il corretto funzionamento degli altri software.

:: Siti e liste

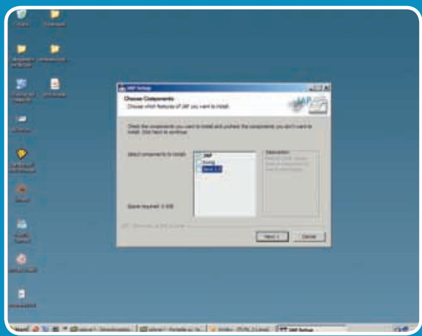
Per dirottare la connessione verso un proxy esistono vari metodi: il più semplice consiste nel raggiungere un sito dal quale, inserendo l'indirizzo delle pagine che intendiamo visitare, accederemo a queste ultime in modalità anonima. Il sito www.anonymouse.org è uno fra i pochi sopravvissuti tra quelli che offrono un servizio simile. A decimare questo genere di servizi sono i costi di gestione e la scarsa simpatia che governi e polizia dimostrano nei confronti di chi mette i bastoni tra le ruote alle attività di intercettazione. La soluzione è rapida da mettere in campo, ma poco pratica: i collegamenti aperti da una pagina "anonimizzata" rimarranno protetti, ma per caricarne una nuova dovremo ripartire dal via. L'altro metodo tradizionale sfrutta l'uso di liste che riportano gli indirizzi di server proxy disponibili a questo uso. Le liste vengono aggiornate ogni giorno, ma spesso comprendono anche server lenti, inefficienti o semplicemente non in grado di mantenere l'anonimato dei loro utenti. Per gestirle, in ogni caso,

COME FUNZIONA

I due schemi rappresentano, con qualche semplificazione, una connessione normale e una anonima. Nella prima, il nostro computer si collega a Internet direttamente e l'indirizzo IP è visibile a qualsiasi server o computer con il quale veniamo in contatto. Nel secondo caso, la connessione "passa" da un server proxy. In questo caso, i server che contatteremo vedranno solo l'indirizzo IP che identifica il proxy, mentre il nostro rimarrà nascosto.

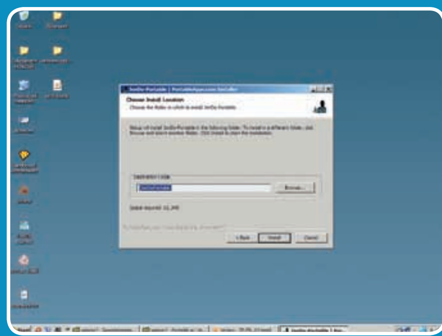


CONFIGURIAMO JONDO



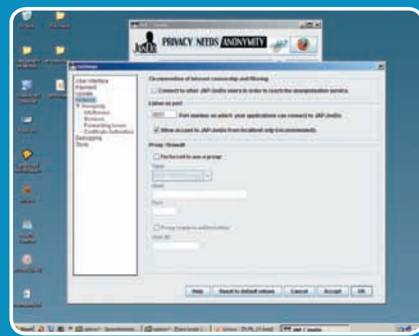
1 JAVA? NO, GRAZIE

La schermata di installazione propone il download della Java Virtual Machine, che però non è sempre aggiornata. Togliamo il segno di spunta e scarichiamo la versione più recente da http://java.sun.com/javase/downloads/index.jsp



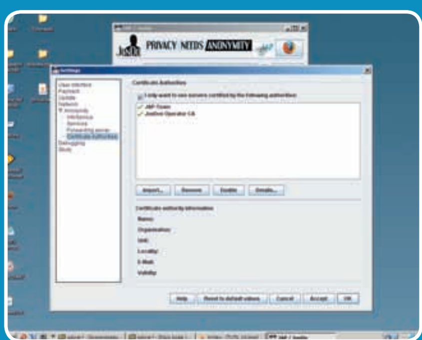
2 ANCHE SU CHIAVETTA USB

Diverso il meccanismo per la versione portabile, comprensiva di tutte le componenti necessarie: basta completare il percorso della directory di installazione, che può trovarsi anche su un supporto esterno che potremo usare su qualsiasi computer.



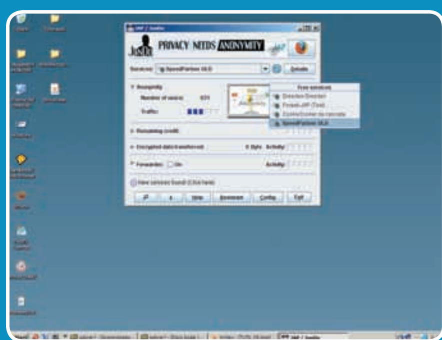
3 SOLO DAL NOSTRO PC!

In Config/Network abilitiamo l'accesso a JonDo solo per il computer su cui è installato scegliendo from localhost only e riserviamogli una porta, che andrà inserita anche nelle impostazioni del browser.



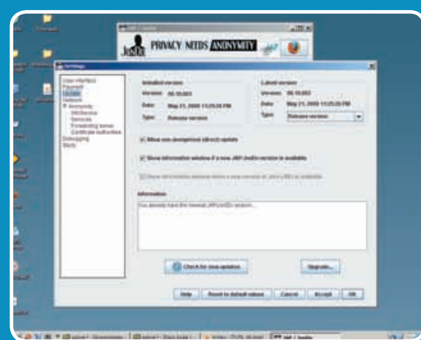
4 SERVER CERTIFICATI

È importante che i server utilizzati siano affidabili. La sezione Certificates Authorities consente di limitare le connessioni ai server selezionati dagli stessi sviluppatori del programma. Una buona garanzia di affidabilità.



5 GRATUITI E A PAGAMENTO

L'interfaccia principale ospita il menu a tendina dal quale indicare il server o il mix di server che vogliamo usare per la connessione. Usiamo quelli gratuiti dalla voce Free services e controlliamone il livello di velocità e sicurezza.



6 SEMPRE AGGIORNATO

La sezione Update ci avvisa quando viene rilasciata una nuova versione, consentendoci di avviare l'installazione. Vengono segnalate anche le versioni Beta, ma è meglio non usarle fino a quando non saranno convertite in versione definitiva.

occorrono applicazioni dedicate come ProxyWay e una buona dose di pazienza.

:: Dalla Germania con Java

Fortunatamente sono disponibili soluzioni un po' più "a misura d'uomo" come JAP, http://anon.inf.tu-dresden.de/index_en.html, nel frattempo ribattezzato JonDo: l'unico requisito per il suo funzionamento è la presenza della Java Virtual Machine di Sun nella versione più recente, onde evitare pericolosi bug di sicurezza. Il programma include una versione di Virtual Machine anche nelle opzioni di download o nella versione portabile, che "gira" anche su supporti esterni. Purtroppo la versione di JVM proposta non è sempre aggiornata, il che suggerisce di ricorrere a queste modalità di installazione solo in situazioni di emergenza.

:: Funzioni avanzate

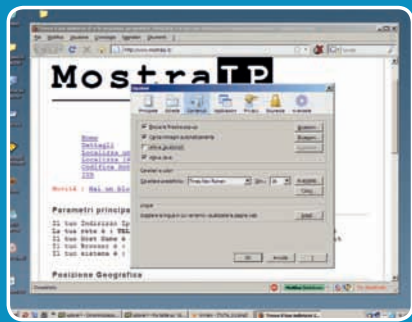
Nato da un progetto delle Università di Regensburg e Dresda, JAP/JonDo supporta numerosi server certificati dal team degli sviluppatori e situati in Germania. Di solito vengono

SAFARI E I PROXY

Sbarcato su piattaforma Windows con versioni Beta a dir poco approssimative, il browser di casa Apple, www.apple.com/it/safari/, sta mietendo consensi sempre più ampi grazie alle sue indubbie qualità, in primo luogo la velocità nel caricamento delle pagine garantita dallo scattante motore di rendering KHTML. La differenza rispetto all'ambiente Mac emerge al momento di accedere alle Preferenze, che su Leopard e predecessori vengono gestite a livello di sistema anziché configurate nella singola applicazione. La memorizzazione di un proxy non era neppure supportata dalle prime versioni, ma è stata introdotta in seguito. Quando le usiamo, però, scopriamo che Safari usa lo stesso sistema di Internet Explorer, sfruttando quindi le impostazioni di Windows esattamente come fa il browser di Microsoft.

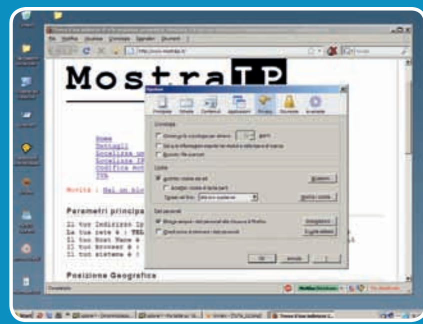


IMPOSTIAMO IL BROWSER



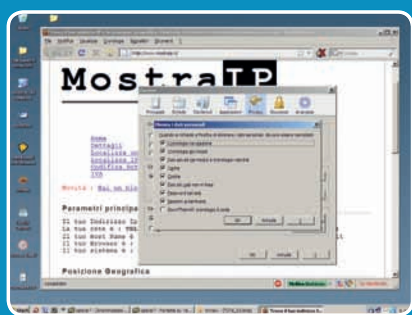
1 ATTENTI AI JAVASCRIPT

Nella sezione Contenuti delle Opzioni scegliamo Avanzate per limitare le funzionalità per i Javascript. Possiamo anche disabilitarli del tutto. Alcuni siti, però, non risulteranno pienamente accessibili.



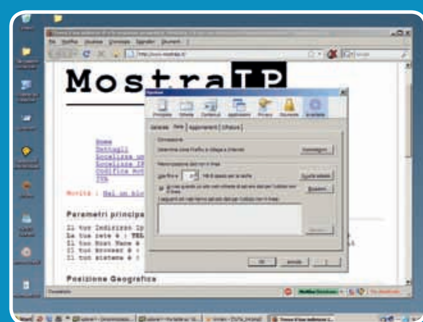
2 STOP AI COOKIES!

Nella sezione Privacy, togliamo il segno di spunta alla voce Accetta i cookie di terze partiJ. In questo modo limitiamo il più possibile la possibilità che rimangano tracce della navigazione.



3 PIAZZA PULITA

Nella stessa finestra, automatizziamo l'eliminazione dei Dati personali alla chiusura del browser selezionandoli da Impostazioni. Non scordiamoci di comprendere anche le estensioni come DownThemAll! .



4 NIENTE PAGINE IN MEMORIA

Nella sezione Avanzate selezioniamo Rete e limitiamo il salvataggio in locale delle pagine visitate riducendo o azzerando la cache e aggiungiamo una spunta anche alla voce dati per l'utilizzo non in linea.

utilizzati nei cosiddetti "mix", ovvero in connessioni che vengono suddivise fra i vari server per rendere ancora più difficile rintracciare il percorso compiuto dai dati. Inizialmente gratuito, ora prevede anche servizi a pagamento, che offrono una maggiore velocità e sicurezza. La qualità dei servizi gratuiti, però, è rimasta più che accettabile. Per configurare il browser basta indicare localhost come host, mentre la porta predefinita da impostare è 4001, per tutti i protocolli. A differenza di altre applicazioni simili, JonDo supporta anche le connessioni tramite FTP.

:: L'alternativa

L'altro "mostro sacro" in questo ambito è Tor, www.torproject.org/index.html.it. Si tratta di un sistema che sfrutta una gestione simultanea di numerosi server e lo smistamento dei dati fra di essi per depistare le cosiddette "analisi del traffico". Nonostante si tratti di un sistema molto evoluto, non è particolarmente diffuso. Non dispone infatti di un'interfaccia grafica e richiede, per interfacciarsi col browser, l'uso di un ulteriore server http. I progetti per la creazione di sistemi più "abbordabili" basati su Tor, come Privoxy, TorCP, Vidalia o Torbutton, hanno mostrato qualche spunto interessante, ma non sono mai approdati alla piena maturità. L'unico software che ha sfruttato in maniera efficace la rete Tor è xB Browser, http://xerobank.com/xB_Browser.php. È una versione modificata di Firefox, basata sulle più recenti release della versione 2 ed equipaggiata per connettersi automaticamente alla Rete Tor senza intervento da parte nostra. ■

Wii HACK

Credevate che il Wii fosse inespugnabile? Beh, vi sbagliavate di grosso!

Quando il Wii fu lanciato sul mercato, furono in molti a dubitare sulle reali possibilità di installare un modchip (efficiente) al suo interno, visto e considerato che Nintendo poteva contare su di un'arma in più rispetto alla scorsa generazione di console: l'aggiornamento del firmware. Oggi, a tre anni di distanza, non solo esistono svariati modchip in commercio, ma è addirittura possibile lanciare codice non firmato senza nemmeno modificare la console. Come? Lo scoprirete leggendo il nostro speciale!

Chiariamo subito una cosa: modificare un Wii non è un'impresa così semplice come potrebbe apparire sulle prime. Non basta, infatti, essere in grado di maneggiare un saldatore e di scegliere un modchip in base alle sue funzionalità, ma occorre conoscere una serie di dettagli fondamentali per evitare di ritrovarsi tra le mani un chip incompatibile. Dal primo modello di Wii immesso sul mercato alle ultime versioni commercializzate di recente, infatti, Nintendo si è ingegnata per mettere il bastone tra le ruote ai produttori (e ovviamente agli installatori) di modchip, operando delle modifiche a livello hardware che coinvolgono il chipset del lettore DVD. In altre parole, esistono sei modelli differenti di Wii (come illustrato nel riquadro "Non sono mica tutti uguali!"), ognuno dei quali mostra delle caratteristiche ben precise che vanno tenute in considerazione quando si decide di modificare la propria console. L'unico sistema certo per sapere quale chipset monti il lettore del vostro Wii consiste nell'armarsi di cacciavite Triwing e smontare il Wii, per poi leggere il codice stampato sul chip del lettore DVD. Esiste tuttavia un altro metodo, che pur non essendo infallibile al 100% consente di conoscere con un certo margine di sicurezza di che modello si tratti: basta sollevare la console, annotare il numero seriale incollato nella parte inferiore dello chassis e riportarlo su questo sito: http://wiitracker.nintendo-scene.com/search.php. Nella maggior parte dei casi, il risultato ottenuto è affidabile, soprattutto nel caso in cui la console non sia stata acquistata in tempi recentissimi (con gli ultimi modelli si ha invece qualche problema, ma se seguite le indicazioni che riportiamo nel riquadro "Che lettore monta il mio Wii?" non dovreste avere troppi grattacapi).
Bene, ora che avete riconosciuto il chipset montato sul vostro Wii, potete individuare facilmente il modchip che fa per voi.



NON SONO MICA TUTTI UGUALI!

I modelli di lettori installati sui Wii presenti sul mercato sono in tutto sei, ma possono essere suddivisi in due famiglie: la prima (che per comodità chiameremo "Tipologia A") comprende i modelli che montano i controller DMS, D2A e D2B, mentre la seconda (Tipologia B), è composta dai modelli con i controller D2C, D2C2 e D2E. Vediamoli nel dettaglio.

TIPOLOGIA A

DMS: Molto semplicemente, il chipset più indicato per accogliere l'installazione di un chip di modifica. Se avete una console di questo tipo siete particolarmente fortunati, perché potete montare quasi tutti i modchip presenti in commercio.

D2A: Altro chipset ottimo, che permette di montare praticamente tutti i modchip in circolazione tranne in WiiNinja (il primo in assoluto ad affacciarsi sul mercato). Insomma, dal WiiKey in poi potete dormire sonni tranquilli.

D2B: Anche con il D2B i problemi di compatibilità sono ridotti all'osso, ma qui insorge un problema ben più grave: alcune varianti di questo chipset presentano i pin tagliati (o meglio, "coperti"), il che rende l'installazione del modchip un'impresa molto complicata e solo alla portata dei più esperti (in altre parole, occorre raschiare il chip per far riemergere i piedini!).

TIPOLOGIA B

D2C: Il peggiore in assoluto. Con questo chipset le cose si complicano davvero, perché le saldature non vanno più fatte sui pin, ma direttamente sul chip. Se il vostro Wii appartiene a questa categoria, vi consigliamo caldamente di lasciar fare a un esperto, altrimenti rischiate di andare incontro a spiacevoli sorprese...

D2C2: è una variante del D2C, con qualche problema di compatibilità in più. Ergo: non tutti i modchip compatibili con la famiglia D2C possono essere montati su chipset D2C2. Fate attenzione e leggete bene la nostra miniguida!

D2E: L'ultimissima versione di Wii messa in commercio, che presenta un chipset leggermente diverso dal D2C2. Se la vostra console appartiene a questa categoria, vi conviene tagliare la testa al toro e buttarvi sul Wasabi.

QUALE SCELGO?

I modchip disponibili per Wii sono una miriade, ed è piuttosto difficile districarsi nella selva dell'offerta senza una bussola (soprattutto se si considera che esistono anche i soliti, dannatissimi, cloni made in China). Proprio per questo motivo, qui di seguito vi proponiamo una lista dei chip più diffusi (e più efficienti) disponibili sul mercato.



TIPOLOGIA A (DMS, D2A, D2B)

CYCLOWIZ (WWW.CYCLOPSWIZ.COM)
Buon chip di modifica della prima generazione (il secondo in assoluto), anche se il primo modello era afflitto da un problema di scomodità: per aggiornare il firmware era necessario ricorrere ad un interruttore posto sulla parte esterna dello chassis. Attualmente, invece, l'aggiornamento può essere eseguito tramite DVD.

WIIKEY (WWW.WIIKEY.CN)
Fino a qualche tempo fa, il WiiKey era sicuramente il miglior chip di modifica per Wii presente sul mercato: facilmente configurabile, stabile e in grado di far girare tutti i titoli PAL senza problemi di sorta. Inoltre, il WiiKey è stato uno dei primi chip aggiornabili mediante DVD, un dettaglio che ha sicuramente contribuito alla sua diffusione. Se avete una console della prima generazione, questo modchip rappresenta una delle soluzioni migliori. Il rovescio delle medaglia è rappresentato dalla presenza sul mercato dei soliti cloni fabbricati in Cina, che sono sempre più difficili da individuare.

WIINJA (WWW.WIINJA.COM/INDEX.PHP?CONTAIN=FEATURES)
E' il primo modchip ad essere stato lanciato sul mercato, ed è decisamente performante ed affidabile, ma è compatibile solo con i primi modelli di Wii (quelli che montano il chipset DMS e D2A), e pertanto non ha riscosso un gran successo di pubblico. L'ultimo modello disponibile (il Wiinja Deluxe) è upgradabile (sempre via DVD) e pure in grado di leggere i giochi import (cosa che col modello normale non era possibile).

TIPOLOGIA B (D2C, D2C2)

ARGON (WWW.INFECTUS.BIZ/ARGON.PHP)
Sviluppato dal team Origa, Argon è una variante di Infectus, il chip di modifica "multipiattaforma" che ultimamente sta riscuotendo molto successo. Questo chip è accompagnato da una cattiva nomea dovuta a una serie di problemi di instabilità riscontrati nella prima versione messa in commercio, ma con l'aggiornamento disponibile attualmente si ha un chip affidabile, che può essere montato piuttosto facilmente anche su chipset D2C2. Unica possibile controindicazione: va aggiornato con un programmatore esterno.

NB: I modchip della tipologia A non sono compatibili con le console che montano un lettore della tipologia B, ma in caso contrario spesso le cose funzionano.

D2CKEY (WWW.D2CKEY.COM)
Questo chip è stato studiato appositamente per i modelli D2C e quindi non è compatibile con nessun altro tipo di console. Il chip è in grado di far girare tutti i giochi disponibili sul mercato, ma la sua installazione richiede l'uso di oltre 30 fili, e pertanto è vivamente consigliato lasciar fare a mani esperte. Insieme al D2Pro, il D2CKey rappresenta una delle soluzioni migliori per chi abbia una console che monta un lettore della famiglia D2C.

D2PRO (WWW.D2PRO.COM)
Dallo stesso team che ha creato il D2CKey, il D2Pro ha il vantaggio di essere "region free" e quindi in grado di leggere anche i titoli import. Nella versione V2, il D2Pro può essere montato anche su una console con lettore D2C2, e più in generale può essere upgradato attraverso un semplice DVD.

D2SUN (WWW.D2SUN.COM/)
Il D2Sun è uno dei chip più economici, ma rappresenta comunque un'ottima scelta: è di facile installazione, è region free e, soprattutto, è compatibile con gli schizzinosi chipset D2C2. Esiste anche la possibilità di aggiornarlo, ma in questo caso occorre un programmatore.

WASABI (WWW.WASABI.NET.CN)
Questo (ottimo) chip non ha nulla da invidiare alla concorrenza, e quanto a funzionalità risulta piuttosto simile al D2Pro, ergo: aggiornamento tramite DVD e compatibilità con i lettori della famiglia D2C2. Il vantaggio del Wasabi, però, sta nella sua compatibilità con tutti i modelli di Wii esistenti.

CHIP "OPEN SOURCE"

Oltre ai chip citati poc'anzi, che sono "pronti all'uso", esistono dei modchip "open source" che vanno preprogrammati, ma che spesso e volentieri mostrano delle potenzialità aggiuntive. Tra questi troviamo: Yaosm, Open Wii, WiiC, WiiREZ, Wiip e Chiip (giusto per citare i più diffusi).

CHE LETTORE MONTA IL MIO WII?

Come già anticipato nel testo, l'unico modo sicuro per scoprire quale modello di lettore DVD si nasconda nella vostra console è quello di smontarla. Il sito che vi abbiamo segnalato è affidabile per buona parte dei modelli, ma con quelli della famiglia D2C2 spesso e volentieri fa cilecca. Ecco un metodo "empirico" per cercare di capire quale sia il vostro chipset.



- Se il numero seriale della console è compreso tra LEH 100XXXXX a LEH 1087XXXX, allora il chipset dovrebbe appartenere alla famiglia DMS/D2A.
- Se il numero seriale è compreso tra LEH 1097XXXX e LEH1356XXXX si tratta quasi sicuramente di un lettore D2B (tenete presente che se il codice è superiore a LEH1233XXXX, quasi sicuramente si tratta del chipset con i pin tagliati!).
- Se il numero seriale è superiore a LEH1400XXXX, ma inferiore a LEH183XXXXX il chipset del lettore è SICURAMENTE un D2C.
- Se il numero seriale è superiore a LEH183XXXXX, quasi certamente si tratta di un D2C2 (o di un recentissimo D2E).

COME TI AGGANCIO IL CHIP

Se sapete come si usa un saldatore, ma l'idea di lavorare direttamente sulla scheda non vi convince del tutto, esiste un rimedio che sembra fatto su misura per voi: si chiama Wii-Clip (www.wii-clip.com) ed è una sorta di adattatore su cui va saldato direttamente il modchip (scongiurando così il pericolo di rovinare la motherboard) e che va poi agganciato alla scheda madre. L'operazione è piuttosto semplice da eseguire, e con una piccola spesa si ha la sicurezza di non compromettere irrimediabilmente la console. Attenzione, però: può capitare che il Wii-Clip si sganci, e in quel caso bisogna smontare di nuovo il Wii per rimetterlo a posto.

OCCHIO AGLI IMPORT

Una regola fondamentale da tenere bene a mente nella maggior parte dei casi: se dovete aggiornare il firmware della console, fatelo attraverso internet o con un titolo PAL (ovviamente, si dà per scontato che il vostro Wii sia europeo), perché upgradando con un gioco USA/JAP correte il serio rischio di "brickarla" (ovvero di "bloccarla").

:: Il backup, questo sconosciuto



Ora che avete scoperto quale chip fa al caso vostro, vi serve conoscere gli strumenti da utilizzare per creare le vostre copie di backup senza farvi venire troppi mal di testa. Prima di tutto dovete creare un dump (ovvero una sorta di "immagine") del gioco, che andrà poi masterizzato utilizzando un programma freeware. A questo proposito, occorre ricordare che il programma che andrete ad utilizzare per creare il dump (Rawdump), non è in grado di riconoscere il contenuto di un DVD per Wii con qualsiasi lettore, ma solo con alcuni modelli precisi: gli LG serie 8161-b, 8162-b, 8163-b e 8164-b funzionano perfettamente, e pare che anche alcuni modelli di Hitachi (serie GDR) si prestino per l'operazione. Se non disponete di un lettore DVD di questo modello, comunque, potete sempre creare la copia di backup direttamente su Wii (o meglio, su scheda SD), ma in questo caso il processo è piuttosto laborioso (se siete interessati, comunque, su internet trovate delle guide che illustrano tutti i procedimenti da seguire). Dopo aver scaricato e scompattato Rawdump 2.0 (lo trovate a questo indirizzo: http://wiki.gbatemp.net/wiki/index.php?title=RawDump#Download), installate le librerie di .NET Frameworks 2.0 e riavviate il computer. A questo punto, aprite il programma (cliccando su Rawdump.exe), inserite il disco del gioco originale per Wii nel lettore DVD del PC (sui cui, lo ricordiamo, deve essere installato Windows XP), e selezionate la voce relativa al vostro lettore: apparirà una schermata che indica il contenuto del disco. Cliccate su "Start Dump" e il processo di dumping (che dura circa 2 ore e mezza) avrà inizio. Una volta terminata l'operazione, occorre controllare se il dump è andato a buon fine, verificandone le dimensioni: se il file "pesa" 4.37 GB (4,699,979,776 bytes) siete a cavallo, altrimenti vi toccherà ripetere l'operazione da capo. Quando il dump è pronto, rimane solo l'ultimo passaggio: la masterizzazione del file ISO ottenuto. Il nostro suggerimento è quello di adoperare ImgBurn (http://www.imgburn.com/) , e di settare la velocità di masterizzazione a 4X/6X (qualcuno arriva anche a 8X, ma potrebbe non funzionare con alcuni modelli di masterizzatori). Per quanto riguarda i supporti, i Verbatim (DVD –R) sono universalmente riconosciuti come i migliori, ma ricordate che alcuni lettori prediligono il formato DVD +R (è sufficiente fare qualche esperimento e controllare quale copia di backup viene letta meglio dalla vostra console). Assicuratevi infine che il vostro masterizzatore sia aggiornato con l'ultimo firmware disponibile e che durante la masterizzazione non ci siano altri processi attivi che potrebbero rallentarla, et voilà: il gioco è fatto!





Il Chiip è in assoluto uno dei migliori modchip "open source" presenti sul mercato.

:: La scena HOMEBREW



Come per tutte le console che, in qualche modo, sono state "bucate" dagli hacker, anche attorno al Wii si è pian piano sviluppata una florida scena "homebrew" (con il termine "homebrew" si allude a quei programmi "fatti in casa" dagli utenti), che da qualche mese ha cominciato a dare i suoi frutti. Uno degli esperimenti più interessanti in questo senso si chiama "Twilight Hack" e permette di lanciare codice non firmato senza nemmeno modificare la console. Con questo trucchetto si possono far girare giochi originali di importazione (niente copie di backup, però: per quelle



Per smontare il Wii occorre un cacciavite Triwing come questo: fate attenzione ad alcuni modelli che si trovano su Ebay, che si squagliano come burro dopo qualche utilizzo!

serve comunque un modchip!), oppure installare canali, programmi homebrew e giochi della Virtual Console. Si tratta essenzialmente di un salvataggio modificato di Twilight Princess in grado di sfruttare un bug del gioco per creare un buffer overflow, e consentire in questo modo di lanciare codice personalizzato. In realtà, il Twilight Hack era stato bloccato dall'ultimo aggiornamento del firmware della console (il 3.3), ma gli inventori si sono ingegnati e sono riusciti a superare anche questo ostacolo. Per evitare di ripetere ogni volta l'operazione, esiste addirittura la possibilità di installare sulla dashboard un canale personalizzato, il cosiddetto "Homebrew Channel", il quale verrà utilizzato tutte le volte che si voglia accedere a del codice non firmato. L'ultima versione del Twilight Hack e tutte le istruzioni su come utilizzarlo sono a questo indirizzo: http://wiibrew.org/wiki/Twilight_Hack. Se invece volete installare l'Homebrew Channel tutto il materiale che vi serve è qui: http://wiibrew.org/wiki/Homebrew_Channel.

:: Questione di import

Come già anticipato qualche pagina fa, per evitare il famigerato brick della console non bisogna mai e poi mai aggiornare il firmware utilizzando un gioco di importazione. Tenendo ben presente questa nozione, si possono tranquillamente utilizzare anche i giochi USA e JAP su una console PAL. Per alcuni titoli, però, subentra un problema di incompatibilità con il formato video (NTSC da una parte e PAL dall'altra), e quindi il gioco non vuole proprio saperne di partire. Per aggirare quest'ostacolo, si può ricorrere a due soluzioni: acquistare il Free Loader di Datel (in questo caso, però, la console non deve essere stata aggiornata all'ultimo firmware, il 3.3, che di fatto blocca il Free Loader) oppure utilizzare un homebrew chiamato Gecko Region Free (lo trovate qui: http://wiibrew.org/wiki/Homebrew_apps, nella sezione "Loaders").





:: Un programma truccato

Da Super Mario Galaxy in poi, Nintendo ha adottato un sistema di protezione in grado di rilevare se il gioco inserito nel lettore del Wii è un originale oppure una copia di backup. Se si tenta di avviare un backup di Mario Galaxy, insomma, la console lo rileva, viene visualizzato un messaggio d'errore ("Errore 001: dispositivo non autorizzato) e il gioco non parte. Anche per questo inconveniente, però, c'è una soluzione: un programmino per Windows in grado di leggere il contenuto di un file ISO e di modificarlo a piacimento. Il nome del software è Trucha Signer (http://www.ingenieria-inversa.cl/files/trucha021.rar), e permette di compiere operazioni di varia natura, oltre ovviamente a rimediare all'errore di cui sopra. Per esempio, può essere impiegato per patchare un gioco NTSC (tramite un altro programma chiamato Video Mode Changer), per modificarne la lingua oppure per ridimensionarne la grandezza, in modo da far star tutto su un DVD5 (un'opzione che si rivela utilissima con Smash. Bros Brawl).

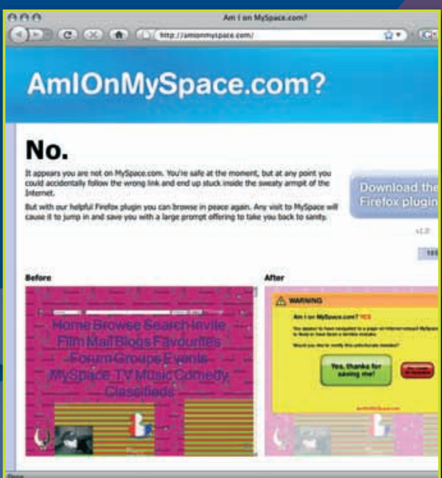
ATTENZIONE, ATTENZIONE!!!

Come tutti voi dovreste ben sapere le procedure riportate in questo articolo sono assolutamente illegali e, come se non bastasse, ogni intervento non autorizzato dalla casa madre sul vostro hardware porta all'immediata invalidazione della garanzia. Come al solito non non vi abbiamo risparmiato nessun trucco ma vi ricordiamo che tutto questo ha senso e scopo solo educativo e sperimentativo.

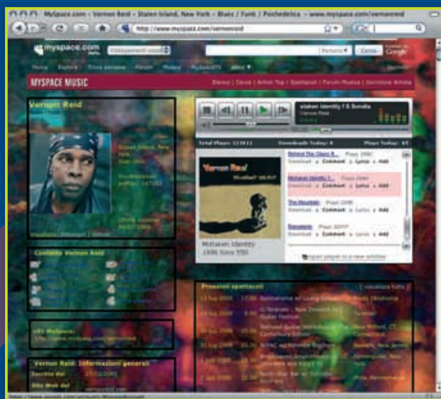
Come evitare MySpace (e vivere felici)

Ovvero: un'estensione per salvare la nostra anima (e la nostra vista) dal social networking di cattivo gusto

Evitare MySpace? Nulla di più facile grazie ad un plugin per Firefox che si chiama "Am I on MySpace.com?"(http://amionmyspace.com/). Se si capita (ovviamente per sbaglio) sul famigerato sito web l'estensione ci offre subito la possibilità di abbandonarlo per lidi meno ameni.



Non rientrerà tra le dieci (e nemmeno cento) aggiunte fondamentali per navigare meglio sul web ma è una soluzione pratica e anche divertente per chi non è abbastanza attento o non sa come modificare il proprio file hosts. Un modo per evitare l'imbarazzo e soprattutto la visione di quegli offensivi sfondi psichedelici che paiono essere la norma sugli account di MySpace. Li usa anche il mio chitarrista preferito, guarda un po'.



:: Installiamola

La homepage di "Am I on MySpace.com?" è chiarissima nello spiegare cosa faccia l'estensione. L'installazione si fa con un click sul pulsante "Download the Firefox plugin" oppure andando su http://amionmyspace.com/install.html



Comparirà una finestra: diamo l'approvazione e poi sarà necessario chiudere il browser e riavviarlo. Aggiungiamo una cosa scoperta a nostre spese: l'estensione non è compatibile con il nuovo Firefox 3 quindi bisognerà usarla con la versione 2 del browser open source, tuttora disponibile (http://www.mozilla.com/en-US/firefox/all-older.html) e che verrà aggiornata fino a dicembre di quest'anno.



:: In azione!

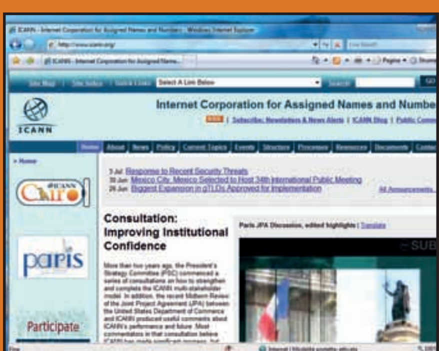
A questo punto non resta che provare l'efficacia andando "casualmente" su una pagina qualsiasi di MySpace.com . Il caricamento verrà interrotto e vi si sovrapporrà un velo con un avviso che recita in inglese "Sono sun My Space? Sì - Sembra che tu abbia navigato su una pagina della fogna MySpace.com di Internet . È probabilmente un terribile sbaglio. Vuoi porre rimedio a questa spiacevole situazione?"
Sotto ci sono due pulsanti: uno, più grande, torna indietro al sito che stavamo guardando poco prima. Il secondo conferma che vogliamo restare su Myspace. A voi la scelta.

Nicola D'Agostino

DSN, questi sconosciuti

Come funzionano e come possono diventare fonte di rischio

Non è solo questione di fortuna. Quando cerchiamo un sito Internet e magari ne conosciamo appena il nome o il contenuto, dobbiamo solo utilizzare un qualsiasi motore di ricerca per veder comparire davanti ai nostri occhi una lista di indirizzi possibili, compreso, nella maggior parte dei casi, quello che cercavamo. Facile e veloce, almeno così sembra. In realtà, le logiche che regolano l'assegnazione dei nomi dei domini e la relativa gestione è ben più complessa di quanto sembri apparentemente e sono molti i passaggi che i nostri computer devono eseguire prima di poterci portare alla pagina Web che ci interessa.



GESTIONE CENTRALIZZATA
L'ICANN, www.icann.org, oltre ad assegnare gli indirizzi IP si occupa di molte altre attività: identifica i protocolli di rete, gestisce i nomi di dominio di primo livello e si occupa anche dei Root Server.

:: Codice identificativo

Ogni computer che appartiene a una rete deve essere immediatamente identificabile e riconoscibile. Questo per permettere a qualsiasi altro dispositivo della stessa rete, o di una rete diversa nel caso di connessioni esterne, di poter inviare e ricevere dati senza che si verifichino problemi o perdite di informazioni. L'identità di un PC collegato a una rete viene stabilita tramite l'assegnazione di un codice *IP*, ovvero *Internet Protocol*, che ha una funzione simile a quella di un classico indirizzo stradale. Così come l'indirizzo di una abitazione ne permette l'immediata collocazione all'interno della mappa cittadina, l'indirizzo IP consente di identificare il dispositivo che ci interessa all'interno della rete. Purtroppo, mentre l'indirizzo stradale è univoco ed esiste un'unica abitazione a cui corrisponde, nel caso



OGNI COSA AL SUO POSTO
Gli indirizzi IP possono essere visualizzati graficamente come elementi di una struttura che prende il nome di Standard ISO/OSI. Come si vede, il protocollo IP agisce a livello di Rete.

dell'indirizzo IP si possono verificare molte situazioni differenti: un computer, infatti, può cambiare indirizzo IP per vari motivi e molto spesso la semplice conoscenza dell'IP assegnato a un PC non è sufficiente per risalire al suo proprietario.

:: Dentro le logiche

Attualmente gli indirizzi IP che vengono gestiti dalla maggior parte dei sistemi operativi sono di tipo *IP4*. Il numero *4* inserito al



GIÀ PRONTO
Per sapere a chi appartiene uno specifico nome di dominio, basta consultare il database Whois. Dal sito del NIC, www.nic.it del CNR di Pisa, dobbiamo solo entrare nell'apposita sezione.

termine della sigla IP indica che l'indirizzo stesso è composto da quattro elementi distinti separati da un punto. Tornando all'esempio dell'indirizzo stradale, quando desideriamo mandare una lettera a un amico o a un conoscente dobbiamo scrivere sulla busta una lunga serie di indicazioni: il nome del destinatario, la via e il numero civico, il CAP, la città e la provincia di destinazione. Un IP4, analogamente, è composto da quattro parti differenti che assolvono al compito di identificare, fra tutti quelli collegati alla rete o a Internet, solamente il computer che ci interessa. Ogni elemento di un indirizzo IP4 è costituito da un numero compreso fra *0* e *255*, cioè da un valore numerico corrispondente a uno degli stati associati a 8 bit. Un classico esempio di indirizzo IP4 utilizzato all'interno di una rete domestica è rappresentato dalla seguente serie di numeri: *192.168.0.1*

:: Un mondo complesso

Non tutti gli indirizzi IP sono dello stesso tipo e ne esistono differenti tipologie sia in base al tipo di impiego che ne viene fatto sia in relazione alla loro modalità di funzionamento. Nel primo caso, è possibile distinguere due gruppi diversi di indirizzi: quelli *pubblici* e quelli *privati*. Per chiarire cosa sia un *IP pubblico* dobbiamo sapere che i primi due elementi di ogni IP4 sono, in realtà, due numeri che identificano un intera *famiglia* di indirizzi. Per esempio, tutti gli IP4 da *82.59.0.0* a *82.59.255.255* sono assegnati a un unico operatore di telefonia, *Tim, www.tim.it*, che li utilizza in modo "pubblico" assegnandoli ai propri clienti. Un *IP privato*, invece, risulta utilizzabile e visualizzabile solo all'interno della rete nella quale viene definito. Un'ulteriore classificazione degli indirizzi IP è quella che li suddivide in *statici* e *dinamici*. Con il termine di *IP statico*, si indica un indirizzo IP che ci viene fornito da un provider per la connessione a Internet e che non viene mai modificato anche scollegandoci e collegandoci ripetutamente. La maggior parte delle connessioni utilizzate in ambito domestico, al contrario, sfrutta *IP dinamici* che vengono assegnati di volta in volta al computer dal gestore di telefonia.



DNS e non solo
Gli attuali server DNS, come il modello DNS-323, D-Link, www.dlink.com nella foto, affiancano al loro principale utilizzo anche molte altre funzioni che li rendono prodotti completi e versatili.

:: Dai numeri ai nomi

Quando decidiamo di visitare un qualsiasi sito Internet, quindi, stiamo in realtà collegandoci a un computer, contenente le pagine HTML che ci interessano, contraddistinto da uno specifico indirizzo IP. Se dovessimo inserire nel browser la serie di numeri che costituisce l'IP4 della pagina Web cercata, la navigazione risulterebbe molto più complessa e difficoltosa. Per questo motivo è stato deciso di associare a ciascun IP4 pubblico un corrispondente *nome di dominio* facilmente memorizzabile. Il nome di dominio, per esempio *www.sprea.it*, è generalmente composto da tre parti. La prima, il *www*, indica la modalità di connessione: in questo caso *World Wide Web*. La seconda, sprea, è semplicemente il nome dell'azienda o del-

A CIASCUNO IL PROPRIO

I indirizzi IP pubblici sono rilasciati e regolamentati da uno speciale ente che opera a livello internazionale: l'ICANN, ovvero Internet Corporation for Assigned Names and Numbers. L'ICANN è una struttura no profit, creata nel settembre 1998 per gestire e unificare tutte le attività connesse all'assegnazione dei domini che in precedenza erano realizzate da altre, differenti, organizzazioni. A livello di ogni singola nazione, poi, l'ICANN rilascia a un'organizzazione presente sul territorio e solitamente gestita dall'università, il compito di occuparsi della registrazione dei domini locali. In Italia questo ruolo è svolto dal NIC, www.nic.it, gestito dall'Istituto di Informatica e Telematica del CNR di Pisa.

Classi	32 bits			Intervallo di indirizzi
A	0	Rete	Host	Da 1.0.0.0 a 127.255.255.255
B	10	Rete	Host	Da 128.0.0.0 a 191.255.255.255
C	110	Rete	Host	Da 192.0.0.0 a 223.255.255.255
D	1110	Indirizzo Multicast		Da 224.0.0.0 a 239.255.255.255
E	11110	Riservati per uso futuro		Da 240.0.0.0 a 247.255.255.255



PROTEZIONE AL MASSIMO
Per essere certi che i server DNS privati non subiscano attacchi informatici, è necessario installare degli specifici programmi, come DNSSEC, www.dnssec.net, che ne controllano il corretto funzionamento.

Sicurezza a rischio

Fra i vai server DNS esistenti, alcuni, chiamati "open recursive", consentono ai malintenzionati di portare un nuovo tipo di attacco ai nostri computer: il DNS Poisoning o avvelenamento del DNS. Questi server, infatti, contrariamente a quanto fanno i normali server DNS, permettono l'accesso alle richieste di risoluzione provenienti da qualsiasi computer connesso a Internet senza alcun tipo di controllo o di verifica. In questo modo è possibile sfruttarli per reindirizzare gli utenti che stanno cercando di collegarsi a un particolare sito verso una copia identica dello stesso che però viene utilizzata per trafugare dati personali, codici di accesso e password di qualsiasi tipo. Purtroppo, sono già attivi virus e malware in grado di modificare le impostazioni dei server DNS su Windows per reindirizzarli verso quelli contraffatti. Chi utilizza Windows Vista, però, ha a disposizione uno strumento di sicurezza ulteriore: la tecnologia User Account Control, appositamente studiata per avvisare l'utente su qualsiasi modifica venga apportata al sistema.

l'ente che detiene i diritti del dominio. La terza, in questo caso it, prende il nome di *suffisso* e può attualmente appartenere a tre differenti categorie: *nazionali, commerciali* o relativi a organizzazioni.

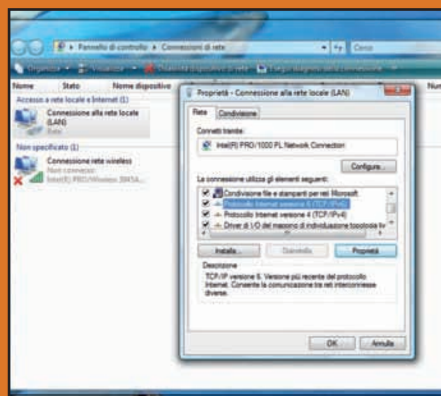
:: Tutto in automatico

Il compito di trasformare il nome di dominio nel corrispondente indirizzo IP4, oppure IP6, viene svolto da una serie di computer che prendono il nome di Server *DNS*. La sigla *DNS*, formata dalle iniziali dei termini Domain Name System, indica proprio il *sistema di assegnazione dei nomi dei domini.* L'operazione che permette di convertire un nome in un indirizzo viene detta *risoluzione* DNS mentre quella contraria, che consente il passaggio dall'indirizzo IP al nome corrispondente, viene definita come risoluzione inversa. Ogni volta che utilizziamo il nostro browser per navigare nel 24Web, inoltriamo al server DNS del nostro provider Internet una richiesta di risoluzione DNS. Il Server DNS, allora, controlla nella propria memoria, chiamata cache, se ha le informazioni che stiamo cercando. In caso contrario inoltra la richiesta ai server DNS a lui collegati che, a loro volta, ripetono la procedura di verifica. Se anche gli altri Server DNS non hanno l'informazione richiesta, viene contattato uno dei tredici *Root Server* distribuiti nel mondo. I Root Server gestiscono direttamente le estensioni dei nomi di dominio e comunicando fra loro, permettono di individuare qualsiasi indirizzo Internet attivo nel mondo

I Signori del Web

Sono solo 13 i Root Server esistenti nel mondo. A loro, direttamente o indirettamente, fanno riferimento tutti i server DNS connessi alla rete. Ecco i loro indirizzi IP4:

a.root-servers.net	198.41.0.4
b.root-servers.net	128.9.0.107
c.root-servers.net	192.33.4.12
d.root-servers.net	128.8.10.90
e.root-servers.net	192.203.230.10
f.root-servers.net	192.5.5.241
g.root-servers.net	192.112.36.4
h.root-servers.net	128.63.2.53
i.root-servers.net	192.36.148.17
j.root-servers.net	198.41.0.10
k.root-servers.net	193.0.14.129
l.root-servers.net	198.32.64.12
m.root-servers.net	202.12.27.33



GIÀ PRONTO
Windows Vista, in tutte le versioni, viene commercializzato già predisposto all'utilizzo del nuovo protocollo IP6. Per verificarlo basta visualizzare le Proprietà della connessione di rete attiva.

:: Dal grande al piccolo

I tredici Root Server sono posizionati geograficamente in differenti posizioni: dieci si trovano in vari punti degli Stati Uniti, 2 sono in Europa, rispettivamente a Londra e a Stoccolma, mentre l'ultimo è attivo a Tokio. Il loro corretto funzionamento è fondamentale per l'esistenza stessa della Rete: se tutti e tredici dovessero essere spenti contemporaneamente, infatti, non sarebbe più possibile navigare in Internet. Dai Root Server, tramite degli appositi file chiamati *root hints*, i dati relativi ai vari domini vengono distribuiti agli altri server DNS geografici che si occupano di gestire i nomi dei computer all'interno dello spazio di loro competenza. Questo sistema permette di rintracciare facilmente, tramite un apposito database detto *Whois* (dall'inglese "Chi è"), i proprietari dei vari nomi di dominio. Esistono più livelli di *Whois* relativi ai vari tipi di dominio e gestiti da un'apposita *autorità di registrazione*. Anche qualsiasi rete domestica o aziendale può utilizzare un proprio server *DNS* per gestire i nomi dei computer che la costituiscono ma si tratta di una scelta che, generalmente, viene adottata sono in presenza di un alto numero di macchine collegate.

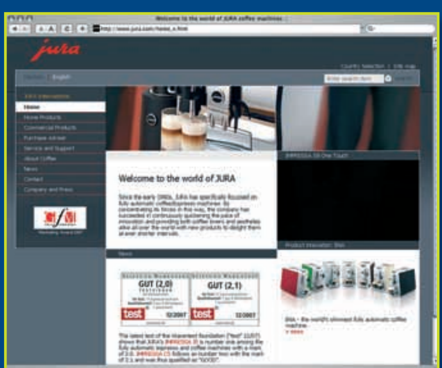
Un ATTACCO... ESPRESSO



Una macchina del caffè che va su Internet, e che rende vulnerabile il PC a cui è collegata? Sogno o incubo di ogni smanettone caffeinodipendente?



L'idea sarà sembrata un colpo di genio ai dirigenti della Jura (http://www.jura.com): un kit di connessione che permette di impostare e controllare le macchine da espresso F9 e F90 a distanza attraverso una connessione di rete. Peccato che questa connessione possa essere sfruttata per accedere al computer con Windows XP che fa da gateway e su cui è in esecuzione il software.
Ma andiamo per ordine.



Nota anche come "Jura Impressa F90 Touch and go!" (http://www.jura.com/de/home_x/products_home_use/f_line/impressa_f90.htm), la Jura F90 è un oggetto mediamente costoso: viene venduto su Amazon a circa 2000 dollari e come pannello di controllo ha un touch-screen attraverso cui scegliere quantità, intensità e temperatura del caffè espresso.

:: Parametri di degustazione

Tra i tanti accessori, insieme a cialde, decalcificatori, compresse per la pulizia c'è anche lo "Jura Internet Connection Kit" o "Impressa Web Pilot" (http://www.jura.com/de/home_x/service_support/expression_symbols.htm?reference=37488&checkSum=5593FCC27261411EE00D4AA14D5FDE3D). grazie a cui la macchina da caffè si collega e può venire "pilotata" da Internet. Il risultato è che si può impostare qualsiasi parametro da remoto, comodamente, e magari andare poi a prelevare la propria tazza di caffè fumante. Altro utilizzo del kit di connessione è per risolvere problemi o guasti: i tecnici della Jura possono infatti effettuare test diagnostici a distanza e consigliare soluzioni senza che l'aggeggio si sposti dalla cucina (o sala). Il sogno di ogni hacker?



:: All your coffee are belong to us?

Per andare in rete però c'è bisogno di un PC con Windows XP alla cui connessione la F9 e F90 si appoggiano, ed è proprio questo l'anello debole del setup. Secondo un messaggio di Craig Wright su Security Focus (http://www.securityfocus.com/archive/1/493387) c'è almeno una backdoor e un utente smaliziato può sfruttare il programma della Jura per impossessarsi del computer con XP. Da sogno di ogni hacker la F90 si trasforma in un incubo di sicurezza: le informazioni fornite sono poche ma Wright afferma che ci sono diverse vulnerabilità e che al momento non è possibile porre rimedio con patch.

Sarà forse meglio continuare ad usare solo la vecchia Bialetti un po' ammaccata?

Nicola D'Agostino

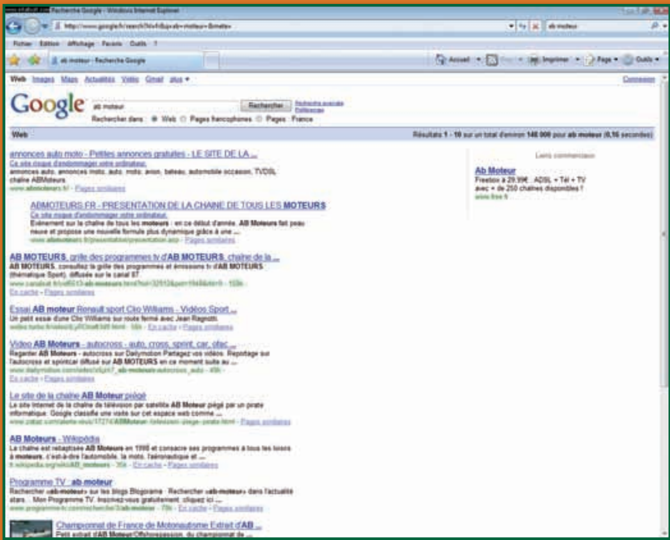


Attacco per conto TERZI

Dopo la diffusione di VIRUS per posta elettronica e tramite programmi offerti su reti peer-to-peer, ecco l'infezione tramite siti Internet di tutto rispetto. Attenzione: a quanto pare, nessuno è al sicuro

Da diversi mesi, una decina di gruppi di pirati particolarmente ben organizzati terrorizza Internet sfruttando un enorme numero di siti ad alto traffico. Nessuno sembra in grado di sfuggire all'attacco. MTV, Durex, MSNBC, nonché vari siti ufficiali del gruppo AB, specializzato nella televisione satellitare. Il sistema di attacco sembra essere semplice e particolarmente efficace. Gli intrusi non mirano a distruggere il sito in cui si infiltrano. Preferiscono un gioco più soft e più insidioso. Per questo si servono di un DIY (Do It Yourself – "fai-da-te", cioè un programma fatto in casa) come Asprox. Asprox, per esempio, utilizza dei DIY che hanno la funzione di inserire comandi SQL (una tattica detta SQL injection) per violare i siti e installarvi comandi dannosi, per esempio programmi-spia.
Il "bot" installa semplicemente un piccolo iframe nel codice sorgente del sito violato e il gioco è fatto. "Per quanto riguarda MTV France" - spiega uno specialista dell'argomento - "le SQL injection di massa sono state individuate ed eliminate rapidamente.

Ciò che suscita preoccupazioni è che le infiltrazioni hanno toccato i due principali flussi RSS e questo ha avuto un

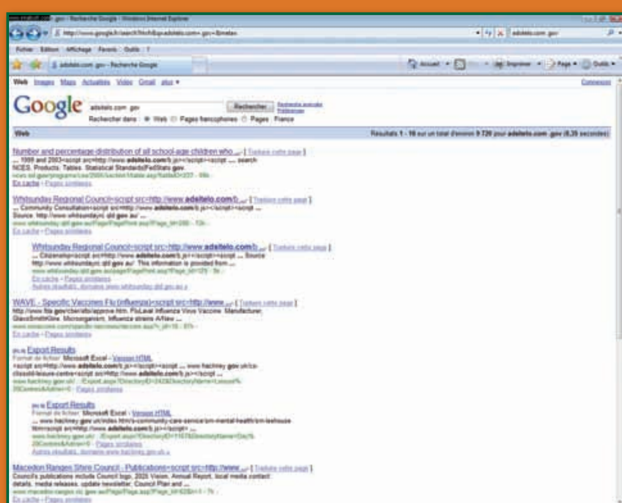


effetto a valanga perché tutti gli utenti dei siti che fornivano le news potrebbero essere stati esposti agli attacchi". In sé, nulla di nuovo: l'episodio dimostra ancora una volta che nessun sito è realmente sicuro. I pirati, tuttavia, hanno capito rapidamente l'importanza di questo tipo di attacchi. Più è noto il sito violato, più numerose saranno le vittime.

:: Eppure eravamo protetti...

A fine maggio, la casa internazionale produttrice di profilattici Durex non immaginava davvero che le sue protezioni avessero una falla. Uno gruppo di pirati era riuscito a inoculare un iframe che avviava lo scaricamento di un programma-spia sui computer dei visitatori. Un attacco pirata totalmente insospettabile per il navigatore, specie se il suo computer e i suoi programmi di navigazione (antivirus, browser, player per flash...) non erano stati aggiornati. Questi attacchi sono particolarmente pericolosi. I pirati sfoggiano una strategia offensiva e una capacità di organizzazione che lasciano senza fiato. Nel caso di Durex, erano stati installati numerosi siti emittenti, che nascondevano completamente il programma-spia. I pirati hanno approfittato a lungo di una falla nel programma Flash Player di Adobe. Si tratta di un punto debole che consente di scaricare un programma-spia sul computer di un visitatore del sito. In occasione dell'attacco di fine maggio, si è scoperto che Durex non era stata l'unica vittima: oltre 10.000 siti diversi erano stati colpiti. Tra le vittime, l'enciclopedia on-line di Microsoft e il sito dell'aeroporto francese di Tolone-Hyeres. Un dato ancor più grave è che alcuni siti Internet di canali televisivi hanno fatto da supporto per questi attacchi. Diverse televisioni satellitari e DTT, come NT1 e AB Moteur del gruppo AB, sono state vittime di queste infiltrazioni. Inutile aggiungere che i visitatori di questi siti non hanno trovato la situazione molto divertente. Un buon antivirus, anche gratuito come Avast, permetteva di rilevare un tentativo di infiltrazione a partire da AB Moteur o NT1. Il collegamento violato rinviava al sito adsitelo.com, sul quale il pirata aveva collocato un programma-spia. Nemmeno le forze armate sono state risparmiate da questo attacco, il che prova l'abilità dei suoi autori. La Camera di commercio e dell'industria di Parigi, la Rete di informazioni sui diritti dell'infanzia e anche un sito dell'esercito canadese sono stati oggetto di tentativi di infiltrazione da parte dei pirati. Lo scenario è il medesimo: bot SQL, iframe maligno installato nei siti presi di mira e server piratati con la funzione di diffondere i cavalli di Troia. Va notato che i pirati avevano predisposto diverse decine di





siti manomessi, tra i quali i più pericolosi erano bigadnet.com, adsitelo.com, advabnr.com, datajto.com e getadw.com.

:: Come difendersi?

Difendersi è a un tempo facile e difficile. Questi pirati hanno sfruttato delle falle denominate comunemente 0dayz: si tratta di vulnerabilità che pochi conoscono. Per tentare di respingere questi attacchi dovrebbero bastare un browser e programmi aggiornati uniti a un firewall e a un antivirus correttamente configurati. Tuttavia, come ci conferma un dipendente di un'azienda di sicurezza informatica: "Questo dimostra ancora una volta che nessun sito è del tutto sicuro". Un lettore ha scoperto che un attacco di questo tipo era partito anche da un sito denominato banner82.com: "È stato il file b.js a mettermi la pulce nell'orecchio. L' infiltrazione SQL era codificata in esadecimale: elencava tutte le tabelle e tutti i campi di testo e aggiungeva un richiamo javascript a questo URL. Nei log si vedevano i cookie dei membri modificati in questo modo, con banner82=update seguito da altre informazioni sul sito". Come abbiamo detto, i pirati non sono mai a corto di idee. ■

Dentro la biblioteca di INTERNET

Come funziona l'Internet Archive, la biblioteca di Alessandria del web. Storia del progetto, hardware e tecnologia, clienti e curiosità



In un'intervista del 2002 con The New Scientist (http://www.newscientist.com/article/mg17623705.000-way-back-when.html) Brewster Kahle ha affermato: "I siti web sono come le sabbie mobili. La vita media di una pagina web è di cento giorni. Dopodiché viene cambiata o sparisce. Quindi tutta la nostra società intellettuale è costruita sulla sabbia".
È per questo che nel 1996 Kahle, che viene dall'MIT ha creato The Internet Archive (http://www.archive.org), un'organizzazione no profit il cui obiettivo è offrire una memoria storica del world wide web a ricercatori, storici e studiosi. The Internet Archive ha aperto ufficialmente solo attorno al 2000 ma in questi anni si è conquistata un posto indiscusso come l'archivio principale non solo di pagine web ma in generale di testi, immagini, musica e video e persino software di importanza storica e culturale.
Una recente intervista (http://news.oreilly.com/2008/06/gordon-mohr-takes-us-inside-th.html) con Gordon Mohr, addetto tecnico in capo, illumina sul funzionamento di questo ciclopico archivio, sui suoi retroscena, partnership e sui meccanismi per gestire tutti quei dati.



IL PETABOX

Uno degli oggetti più affascinanti del datacenter dell'Internet Archive è un rack custom progettato dallo staff interno e pensato per archiviare ed elaborare un milione di GigaByte di informazioni. Gli obiettivi primari erano un basso consumo (6kW per rack), un'alta densità di archiviazione (dai 100 TB in sù per rack), potenza equivalente a 800 PC, resistenza, facile trasportabilità e facile uso anche da un container. Il risultato è il Petabox (http://www.archive.org/web/petabox.php) di cui nell'Internet Archive ce ne sono ormai parecchi e che ha avuto talmente successo che è stata creata un'azienda ex novo per commercializzarli.



:: Gli utenti speciali

L'Internet Archive ed in particolare la Wayback Machine, la sua "macchina del tempo" sono aperti a chiunque ma ci sono anche altri servizi mirati richiesti da utenti speciali. Ad esempio diverse biblioteche e archivi nazionali richiedono copie settoriali a loro utili di parte del web: Mohr cita la Library of Congress statunitense che ha commissionato il crawling di siti di news, governativi e politici ma anche le Biblioteche nazionali dell'Australia, Irlanda, Francia e persino Italia hanno o hanno avuto specifici progetti in corso.

:: Un cluster in crescita

A monte però c'è un'organizzazione che comunque salva il salvabile rima che scompaia: Mohr ricorda che quando un'azienda o un'organizzazione sparisce dopo un po' sparisce anche la sua presenza sul web e quindi tempismo e capacità di archiviazione sono fondamentali.
L'internet Archive come Google ha scelto un approccio poco sofisticato e votato all'economicità e ridondanza. Grosso modo sono impiegati un migliaio di computer organizzati in cluster a gruppi di 40 computer. Ci sono poi 11 rack speciali per gli utenti di cui sopra che hanno ognuno una quarantina di server 1U con quattro dischi. Come dimensione complessiva tutto l'archivio web dal 1996 ad oggi pare occupi circa 1,2 PetaByte ma il cluster è in crescita continua e ogni mese (o meno) viene acquistato e si aggiunge un nuovo rack ed esattamente come a Mountain View si tratta di comune hardware pilotato da software open source o sviluppato internamente che pilota dischi acquistati al prezzo di mercato (o anche meno).
Chi si immagina sofisticate configurazione RAID rimarrà deluso: l'Internet Archive confida nel mirroring a coppie di dischi o di computer.



Datacenter

:: Vantaggi e svantaggi

Mohr evidenzia come per la grandezza del datacenter e l'impostazione poco sofisticata i dati dell'Internet Archive siano in uno stato fluido: c'è sempre qualche computer che si sta spostando o anche rotto e questo è il motivo per cui una ricerca tra i siti web del 2004 può dare oggi un risultato e tra qualche giorno uno diverso, piùo meno ricco.
La sua parte in questo stato transitorio la fanno anche gli upgrade software e del sistema operativo, che è storicamente di tipo Linux. Inizialmente il datacenter usava esclusivamente una versione di Red Hat: da questa si è passati a Debian e oggi quasi esclusivamente a Ubuntu. Proprio l'aggiornamento e parificazione di tutto l'hardware a una versione unica di Ubuntu ha reso indisponibile una buona parte dell'indice della WayBack machine per alcuni giorni.

:: Backup? Ad Alessandria

Un'altra chicca rivelata da Mohr è che l'Internet Archive nella sua sede centrale (a San Francisco) al di là dei suoi migliaia e migliaia di dischi sempre in funzione non ha una copia di sicurezza magari su supporti diversi. C'è però un backup remoto molto molto particolare in... Egitto.
L'internet Archive ha una partnership con la Biblioteca di Alessandria che in due occasioni ha ricevuto una copia completa di tutto quanto accumulato dall'organizzazione di Kahle. È successo nel 2002 e poi, come integrazione, nel 2006. I dati non sono stati trasmessi ma spediti fisicamente con tutti i computer: si è caricato un aereo di computer funzionanti prelevati dal centro dati a San Francisco e trapiantati in Egitto dove sono stati riattivati.
La copia in questo paese ha ovviamente anche ragioni simboliche. La distribuzione e condivisione delle informazioni è un aspetto programmatico e insito nel progetto e il rimando alla mitica biblioteca di Alessandria è palese, sin dal software che archivia le pagine del web che poi finiscono nell'Internet Archive, che si chiama non a caso Alexa.

Nicola D'Agostino

LA MACCHINA DEL TEMPO

Uno degli strumenti più utili dell'Internet Archive, e vera interfaccia della memoria storia del web è la Wayback Machine (http://www.archive.org/web/web.php). Si tratta di un motore di ricerca che recupera e mostra tutte le versioni archiviate di una pagina web in un archivio che al momento conta 85 miliardi di pagine dal 1996 sino ad oggi.



Per fare un "salto nel passato" del web basta digitare un indirizzo e controllare cosa e quanto è disponibile.



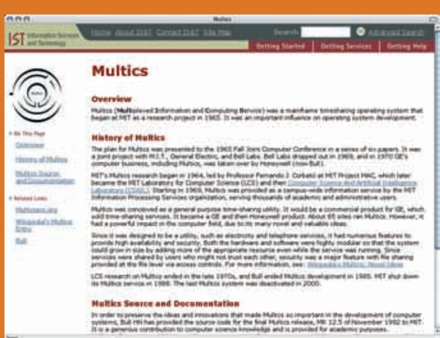
Multics, il nonno di LINUX



Spesso citato ma poco conosciuto, il sistema operativo Multics è diventato "famoso" per aver stimolato la creazione di UNIX ma ha dei meriti indubbi ed una storia lunga e varia che si può finalmente apprendere da una fonte ufficiale. Qualche mese fa la Bull HN, l'ultimo proprietario del sistema operativo, ha deciso di condividere storia, codice altro ancora creando sul web (http://web.mit.edu/multics-history/) un progetto in collaborazione con la prestigiosa Università del Massachusetts, MIT la stessa in cui Multics ha avuto i suoi natali.



Curiosa foto di alcuni degli sviluppatori di Multics davanti alla Honeywell.



Sito Multics.

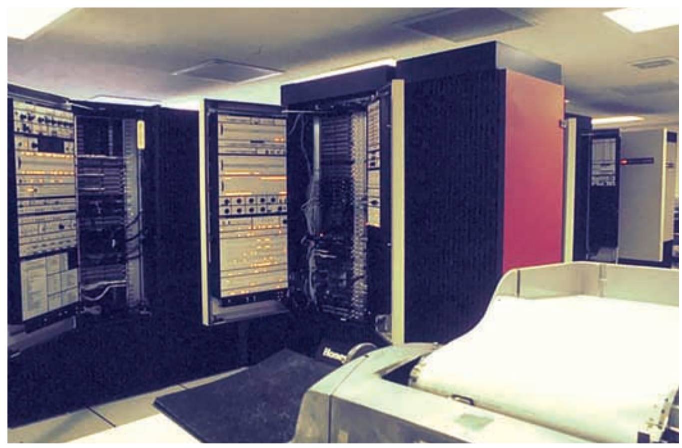
:: Un po' di storia

Multics, che sta per Multiplexed Information and Computing Service è un sistema operativo time-sharing il cui sviluppo è iniziato nel 1964 presso il MIT sotto la guida di Fernando Corbató e in collaborazione con i colossi dell'industria statunitense Bell Labs e General Electric

Multics era sviluppato inizialmente sul maiframe della General Electric, il GE-645 e tra gli sviluppatori c'era Ken Thompson che con l'esperienza su questo computer decise prima per il porting di un gioco e poi per la creazione di un altro sistema operativo meno ambizioso e complesso, Unix, che inizialmente si chiamava Unics con un 'cs' finale che ribadiva -più o meno scherzosamente- il legame di parentela tra i due.



La passione per Multics non ha molti limiti.



Ecco la culla, o meglio, l'incubatrice dove è nato Multics

Multics ha però continuato sulla sua strada tra alti e bassi venendo impiegato con successo commercialmente in decine di enti governativi, aziende e centri di ricerca tra cui l'MIT stesso dove era usato per fini di ricerca e amministrativi. I Bell Labs si ritirarono dal progetto nel 1969 e l'anno dopo anche General Electric decise di abbandonare Multics cedendolo alla Honeywell che già lo supportava sui suoi modelli 6180.

Honeywell ha continuato a sviluppare e commercializzare Multics sino al 1985 e tra i suoi clienti nei primi anni '80 c'era il sistema universitario francese. La consociata Bull se ne è assunta la responsabilità prima in Europa e poi anche negli USA fino al 2000 quando, alla fine di ottobre, è stato spento l'ultimo sistema Multics.

:: I primati

Anche se Multics ha avuto molta meno fortuna rispetto a Unix (con cui ha avuto un rapporto conflittuale) il suo impatto è stato notevole e gli sono riconosciuti anche dai maggiori critici diversi primati.

Multics è stato il primo OS con un filesystem gerarchico: i nomi dei file già negli anni '60 e '70 potevano essere di qualsiasi lunghezza e caratteri. Inoltre file e directory potevano avere più nomi ed esistevano già i link simbolici alla directory.

Altro primato di Multics è il dynamic linking e cioè la possibilità che un processo in corso potesse richiedere e caricare altri segmenti con codice da eseguire, alla bisogna e magari anche in diverse versioni.

Una 'magia' di Multics era la possibilità di riconfigurare l'hardware mentre era acceso. Con il sistema operativo e i processi in esecuzione nonché gli utenti loggati si potevano rimuovere unità centrali, banchi di memoria, dischi ed altro 'a caldo' come diremmo oggi. All'MIT era in auge la pratica di dividere letteralmente i sistemi in due quando non c'era bisogno di molta potenza di calcolo cannibalizzandone uno e costruendo un altro mainframe secondario su cui fare test senza compromettere assolutamente il sistema principale né le operazioni e calcoli in corso di tutti i suoi utenti. Una volta finito il test i vari pezzi venivano gradualmente reintegrati nel mainframe originario.

:: E ci sono anche i sorgenti!

Le risorse per chi volesse indagare su Multics non mancano: segnaliamo perlomeno Multicians (http://www.multicians.org/) che offre anche diversa iconografia e informazioni curiose e folcloristiche.

La parte più bella della presenza ufficiale di Multics su Internet è però che sono stati resi disponibili documentazione e anche i sorgenti. Opportunamente spronata da un dirigente ora in pensione, la Bull un paio d'anni fa si è mostrata illuminata e generosa e ha caricato tutti i file della ultima release di Multics, la MR 12.5 che risale al novembre 1992. Il tutto è disponibile per fini accademici sul già citato sito dell'MIT (http://web.mit.edu/multics-history/source/Multics_Internet_Server/Multics_sources.html) al fine di "conservare le idee e innovazioni che hanno reso Multics così importante nello sviluppo dei sistemi operativi". L'obiettivo finale è di creare un archivio enorme anche per tutte le tesine, ricerche e documentazioni prodotte attorno a questo poco noto 'mostro' dell'informatica.

Nicola D'Agostino

I MITI DI MULTICS

Multics è entrato nella leggenda anche per alcune stranezze, non necessariamente vere. Si tratta dei "miti" raccolti e confermate o smentite su una pagina di multicians.org (http://www.multicians.org/myths.html).
Il mito migliore? Che gli errori di sistema di Multics fossero tutti in latino!
In realtà erano quasi tutti in inglese ma i più (s)fortunati in caso di problemi si sono ritrovati dinanzi a scritte al boot come "HODIE NATUS EST RADICI FRATER". Erano state inserite da Bernie Greenberg, programmatore ma anche musicista e latinista dilettante. La soluzione? Contattare l'assistenza e intanto cercare un dizionario Inglese-Latino per decifrare cosa fosse successo a root, la radice.



Bernie Greenberg: esperto di LISP, hacker e buontempone appassionato di latino